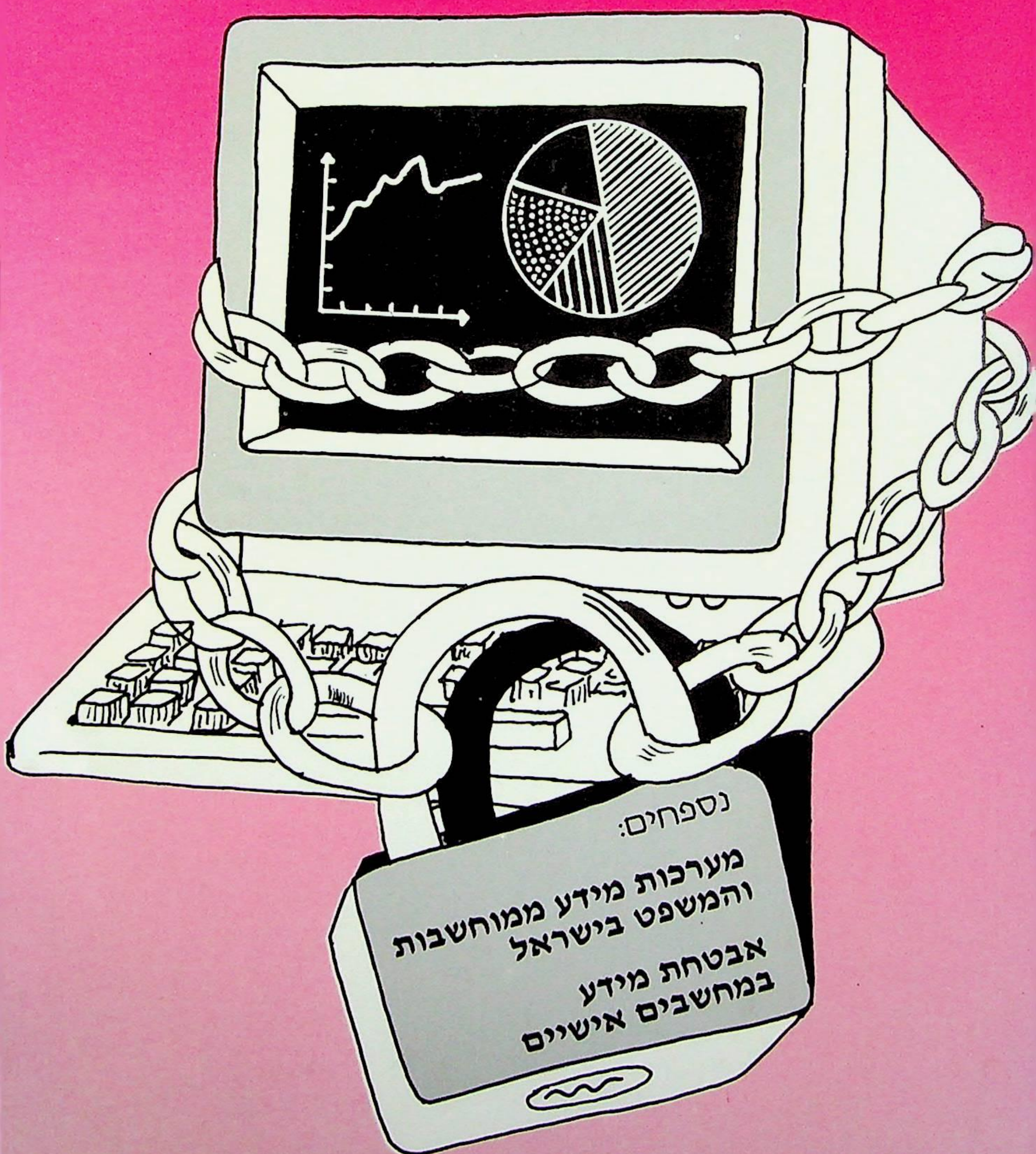
אבטחת מידע במערכות ממוחשבות

ו. פ. ליין



ספרי לימוד והכשרה במדעי המחשב

הוצאת הוד עמי

אבטחת מידע
במערכות ממוחשבות

[illegible]

17/6/90

עורך: יצחק עמיהוד

תרגום: חיים פליבה

אבטחת מידע
במערכות ממוחשבות

ו. פ. ליין

נספחים:

מערכות מידע ממוחשבות והמשפט בישראל

אבטחת מידע במחשבים אישיים

ספרי לימוד והכשרה במדעי המחשב
הוצאת הוד-עמי

Security of Computer Based Information Systems

V.P. Lane

ISBN 0-333-36436-8
ISBN 0-333-36437-6 Pbk

Authorized translation from
the English language edition

הודפס בישראל
אייר תש"ן, 1990
Printed in Israel, 1990

ISBN 965-361-010-4 מסת"ב

תוכן העניינים



פתיחה

למערכות מידע שמבוססות על מחשב יש היום תפקיד חשוב בפעילות העסקית והן חלק בלתי נפרד ממנה. חברות וממשלות מעורבות מדי יום בהעברה אלקטרונית של נתונים רגישים ושל נתונים המייצגים סכומי כסף גדולים מאוד. ללא תלות בשאלה אם הארגון עוסק בהעברת כספים אלקטרונית (Electronic Fund Transfer - EFT), ברור שמידע הוא משאב חשוב ובעל ערך לעסקים קטנים, בינוניים וגדולים. גורם זה ואחרים, כמו תחיקה המחייבת הגנת נתונים, גרמו יחדיו להעלאת נושא אבטחת מערכות מחשב ומערכות מידע המבוססות על מחשב, לדרגת החשיבות שמייחסים לו כיום.

ספר זה מציג שיטות לשילוב האבטחה במערכות מידע המבוססות על מחשב. אין זה ספר הדרכה לאבטחת מחשבים - ספרי הדרכה טובים נכתבו בנושא זה - וגם אין כוונה להשתמש ברשימות תיוג (check lists) כדי להגיע לרמת אבטחה טובה יותר. רשימות תיוג, שנפוצות מאוד בתעשיית אבטחת המחשבים, אינן מובאות בספר, אך אנו דנים בהן ומסבירים אותן כחלק משיטות היוריסטיות לאבטחת מידע.

אחת הבעיות העיקריות של ספרי אבטחת המחשבים היא ההיקף הגדול של הנושאים שכלולים בה, בכללם:

- o אבטחה פיסית של מבנים ומתקני מחשב.
- o הגנה מפני אש.
- o פרטיות.
- o תוכנה.
- o בקרה פיננסית.
- o מחקרים במדעי ההתנהגות של אדם וחברה.

כתוצאה מריבוי הנושאים, נדחקים חלק מהם לשוליים, ללא הצדקה. כמו כן, מומחים שונים תוקפים את הנושא מנקודות מבט שונות. לדוגמה, מומחה אחד יכול להתרכז במקרים של פשעי מחשב, אחר - באבטחה של בסיסי נתונים ושלישי - בחומרה. בכוונתי להקיף בספר זה את הצרכים של אנשי המקצוע שעוסקים בתחומי ניתוח מערכות ואבטחת מידע. כמו כן, אני עונה על הדרישות להכשרה של סטודנטים ששואפים לעסוק בתחומים אלה. באופן טבעי, גם לגישה זו חולשות ויתרונות, אבל ברור שספר זה נותן תמונה רחבה על נושא מורכב מאוד.

מבנה הספר

פרק 1 כולל הגדרות ומינוחים בסיסיים שקשורים באבטחת מערכות מידע המבוססות על מחשב ודיון בחשיבות הנושא. בפרק 2 נמצא את סיכום התפיסות הבסיסיות של אבטחה פיסית. בפרק 3 מתנהל דיון באבטחת נתונים במחשב ובמישק אדם-מכונה, הכולל שיקולים של בקרת כניסה, זרימת נתונים, בקרת ההיקש הלוגי בבסיסי נתונים והצפנה. הנושאים המורכבים העוסקים בחומרה, במערכת הפעלה ובתקשורת מובאים בפרק 4, עם דגש על השפעתם ביישומי מחשב אחרים. פרק 5 דן בתפקידם הקריטי של האנשים באבטחה - כמייצגי איום וכאמצעי הגנה.

בפרק 6 מתוארים הצעדים שיש לנקוט כדי ליצור ולבנות יישום מאובטח. פרק 7 דן בהיבטים התפעוליים של האבטחה ובאופן שבו יכולים נוהלים תפעוליים להבטיח את יציבות רמת האבטחה של יישום המתוכנן היטב. בפרק 8 מוסברות הדרכים לעריכת תוכנית אבטחה לארגון, תוך דיון מורחב בתפקידם המרכזי של האנשים באבטחה - אותו נושא שפותח קודם לכן בפרק 5.

פרק 9 סוקר את הרקע ההיסטורי והבינלאומי של חוקי הגנת הפרטיות והנתונים בבריטניה ומסביר את ההשלכות הניהוליות, הטכניות והכספיות של חוקים אלה. פרק 10 עוסק בצורך באמצעי הרתעה טכניים וחוקיים להגנת זכויות תוכנה. בהקשר זה, מובא דיון בחוקים הבאים: זכויות יוצרים, סודות מסחריים והגנת פטנטים.

בפרק 11 מוצגים מקרים אמיתיים שבהם נתגלו פרצות באבטחה. מקרים אלה מאירים נקודות שונות שהובאו בספר. אחד מאותם מקרים משמש לדיון בתחיקה להגנת נתונים, בעוד שהמקרים האחרים מאירים את החשיבות של תוכנית לשעת חירום (contingency planning), בקרות פנימיות, נוהלים לגיוס עובדים ומדיניות שמגדירה את השימוש שיכולים עובדי מרכז המחשבים לעשות במשאבי המחשב.

פרק 12 מתייחס לצורך בגישה כוללת (הוליסטית) לאבטחה, וסוקר את ההשלכות של השימוש במחשבים אישיים על האבטחה.

הנספח מקביל במידה רבה לפרקים 9 ו-10. הוא מציג נקודת מבט ישראלית בתחום אבטחת המידע ומכיל את תקציר החוק להגנת הפרטיות ועוד.

לספר מצורפות רשימה ביבליוגרפית ואינדקס.

עצות לקוראים

במהלך כתיבת ספר זה חשבתי בעיקר על הקוראים הבאים: אנשי ענ"א המתכוונים להרחיב את תחומי עיסוקם ולהעשיר את תפקידם בארגון וסטודנטים שיתכננו בעתיד מערכות מידע, או שישמשו יועצים לצוות לא טכני של חברה על אבטחת מחשבים. לקוראים אלה יספק הספר מסגרת רעיונית והדרכה לעקרונות ושיטות. עם זאת, ספר זה יכול להועיל גם לכל קורא שיש לו רקע ועניין במחשבים.

בסוף כל פרק ניתנו שאלות שנועדות להקל על הלימוד. רוב השאלות מיועדות ללימוד עצמי, אך ניתן לשלבן גם בדיון בכיתה. חלק מהשאלות מסומנות כשאלות קבוצתיות, שהדרך הטובה ביותר לפתור אותן היא בקבוצה של שלושה עד ארבעה סטודנטים.

עצות לסטודנט

ספר זה נועד לאנשי ענ"א שמתמחים באבטחת מידע, לתלמידי מדעי המחשב, לתלמידי ניהול לתואר ראשון ולאלה הלומדים לתוארים גבוהים. כל הפרקים מתאימים ללימוד, אך ניתן לקרוא כמה מהם כיחידה נפרדת, כמו למשל, הפרקים והנספח שעוסקים בהגנת תוכנה ובתחיקה להגנת נתונים. חפיפה שקיימת בין הפרקים מכוונת להבהיר לסטודנטים ששיטות האבטחה הרבות והשונות משלימות זו את זו, ואין שיטה אחת שיכולה לענות בצורה משביעת רצון לכל בעיות האבטחה.
על המתכננים ללמוד שיטות רבות מתוך פרקים שונים. לפי היגיון זה, החלוקה לפרקים משמשת מעין גבולות מלאכותיים, שיעזרו לקורא להתמודד עם נושא רחב.

הוראה

האבטחה אינה רק נושא מרתק, אלא גם כלי מצוין להדגמת מערכת היחסים שבין אנשים וטכנולוגיה במערכות סוציוטכניות. באופן אידיאלי, על הוראת אבטחה לשקף את האופי הרב-תחומי של עיבוד ואבטחת מידע, ולכן היא מתאימה מאוד להוראה וללימוד בקבוצה.

הכרת תודה

תרשימים 1.1 ו-1.2 נלקחו מתרשים 7 בפרק II של קורס T301 משנת 1984, באוניברסיטה הפתוחה של אנגליה - Complexity, management and change: applying a system approach.

תרשים 3.2 נלקח ברשות מתרשימים 1a ו-1b מהמאמר: "Data security", מאת: Dorothy Dening & Peter Dening, ספטמבר 1979, ACM Computing Surveys. זכויות יוצרים ל: Association for Computing Machinery, Inc.

תרשים 8.2 וטבלאות 8.2 ו-8.3 הודפסו ברשות של המו"ל מתוך המאמר "Security risk management in electronic data processing systems", מאת R.h. Courtney שהוצג ב-AFIPS National Conference בשנת 1977.

תרשים 8.4 נלקח מ- Systems Thinking and Systems Practice, מאת: Peter Checkland. זכויות היוצרים (1981): John Wiley & Sons, Ltd.

טבלה 10.4 הופיעה במאמר: Computing and reform of copyright protection מאת D.J. Grover & R.J. Hart, Computer Bulletin, מרץ, 1982, והיא מודפסת ברשות של British Computer Society.

טבלאות 11.1 ו-11.2 הופיעו ב-Computer Fraud Survey 1985 והן מודפסות ברשות: Controller of Her Majesty's Stationary Office.

הרעיונות לספר זה התגבשו אצלי הרבה לפני שקיבלתי את המשימה לכתוב אותו. ההתעניינות באבטחה החלה בשנות ה-60 המאוחרות, כאשר כיהנתי כמנהל עיבוד הנתונים בקבוצת ג'וזף לוקס והייתי אחראי, בין השאר, לתכנון מערכת משכורות מאובטחת ומערכות פיננסיות אחרות. התעניינות זו התפתחה לאורך שנות השבעים. תחילה, דרך משימות ייעוץ בענפי תעשייה שונים ובסקטור הפיננסי ובהמשך, דרך ניהול פרוייקטים בסקטור הציבורי ולבסוף, במהלך הרצאות בנושאי אבטחה.

בהתנסויות אלו למדתי רבות מאנשים שאיתם עבדתי ואני אסיר תודה לאלה שעזרו, בצורה ישירה ועקיפה, לעבודתי בנושאי אבטחה. אני מודה במיוחד לג'ון קורקורן מ-National Giro Bank; לפרנק דיוויס מחברת שירותי מחשב Littlewood Mail Order; למרק קהרס מהמרכז לחקר מדעי המחשב במעבדות אי.טי.טי-בל בניו-ג'רזי; לג'ון סטפ מ-Audit Consortium בבו־ייטון; לטונברידג' וולס ולאחרים, שקראו חלקים מהספר וסיפקו הערות מועילות. תודתי לפרי לוקופולוס מ-UMIST, שעודד אותי במהלך העבודה על הספר. קיבלתי עזרה מחברים לעבודה בפוליטכניק של צפון לונדון וברצוני להודות להם: אלן צ'יטהם וג'ון פיצ'ים העירו על חלקים מהספר; ביל סמית עזר לי בשימוש במעבד תמלילים; ג'ואן מויה עזרה באיתור הפרסומים וגלוריה שיילר הפיקה את האיורים. ברצוני להודות גם לכמה חברים מהצוות של מקמילן, במיוחד לביל פרי ולמלקולם סטיוארט. ולבסוף, הייתי רוצה להודות לאשתי ג'ואן על התמיכה והעידוד.

פרק 1

איומים, אמצעי הגנה ויעדי אבטחה

האבטחה של מערכות מידע המבוססות על מחשב עוסקת בשיטות להגנת מערכות המידע בפני אירועים עתידיים לא רצויים. שיטות אלו נבחרות על בסיס עלות-תועלת. אירועים אלה, שנתייחס אליהם להלן כ"איומים", יכולים לגרום נזק לארגון ולהוות פרצה ופגיעה באבטחה. אנו יכולים לזהות שלושה סוגי אובדן הקשורים בנתונים:

* אובדן השלימות.
* אובדן זמינות השירותים.
* אובדן הסודיות.

1.1 אבטחה

התפשטות השימוש בטכנולוגיית המידע סיפקה יתרונות משמעותיים. לדוגמה, בקרה טובה יותר של ההנהלה מובילה להגברת היעילות ברמת הארגון. לצערנו, לכל היתרונות האלה תופעות לוואי לא רצויות, שלעתים קרובות קשה לחזות אותן והן עלולות לגרום נזק רב. במקרה שלנו, קיימות הוכחות ברורות לסכנות חדשות שארגונים נחשפים אליהן. לדוגמה, טכנולוגיית המידע תרמה לריכוז של הנתונים ותהליכי עיבוד הנתונים ומכאן - להגברת הסכנה מפני אש. מצד אחר, קיימת נטייה חזקה לכיוון של מחשוב מבוזר, שמגביר את הסיכון מפני התערבות של אנשים בהליכי הקלט והפלט של הנתונים. ארגונים רבים מסרבים להכיר באיומים אלה. הם מוכנים להשקיע סכומי כסף משמעותיים בטכנולוגיית המידע, אך נמנעים מהוצאה נוספת, קטנה יחסית, שתסיר, או שתנטרל, את האיומים. הגורמים הבאים עלולים לגרום לאיומים:

(1) מערכת המידע עצמה - כמו תקלה בתקשורת, או טעות של עובד.
(2) פעולות מכוונות של אנשים.
(3) אסונות חיצוניים, כמו הצפה או ברק.

לאיום הראשון ברשימה משמעות חמורה. יש לבחון את ביצועי מערכת המידע, כדי לקבוע שהמערכת מבצעת פונקציות קריטיות

בסיסיות באמינות וללא תופעות לוואי. מבט זה של האבטחה מקיף את האמינות של הגורמים הבאים: יישומים, מערכת ההפעלה, תקשורת, חומרה וכוח אדם. האנשים הם "לב" אמצעי האבטחה והאיומים כאחד. משתמשים, מנהלים, מתכנתים, מנתחי מערכות, מפעילים ואנשים רבים אחרים מתכננים, מתחזקים ומפעילים את האבטחה של המערכת. אותם אנשים שמעורבים בהכרח במערכת המידע, הם לעתים קרובות החלקים הפגיעים ביותר במערכת.

אנשים מציבים איום מכיוון שהם יכולים לבצע פעולות בשגגה, או במכוון. המתכננים מתחשבים באפשרות של טעויות בשגגה, אך הסכנות הנובעות כתוצאה מפעולות מכוונות וזדוניות מקבלות פחות תשומת לב. מקרה מיוחד הוא מתכננים שעובדים במערכות רגישות ביותר, כמו אלו הקשורות לבטחון לאומי. אסונות חיצוניים אינם מראה נפוץ במרכזי המחשבים, ולכן רק אתרים מעטים מחוסנים מפני אסונות כדוגמת מזג אוויר קיצוני. לאירוע חיצוני כזה עלולה להיות השפעה קטלנית על הארגון. יש לציין שלרוב בעיות האבטחה אין פתרונות אידיאליים.

אפשר להגיע לאבטחה מושלמת בעזרת משאבים אין סופיים, אך למעשה, לא קיימת הגנה מוחלטת בטכנולוגיה המבוססת על מחשבים. המקרים הבאים מדגימים את חוסר האפשרות להגיע לאבטחה מושלמת:

(1) ב-1982 הצליח פורץ לא מקצועי לעבור דרך כל קווי ההגנה של ארמון בקינגהם באנגליה ולהכנס לתוך חדר השינה של המלכה אליזבט.
(2) ב-1983 הצליח נער אמריקני להתחבר למחשב של לוס-אלאמוס.
(3) ב-1984 הצליחו פורצי מחשבים להכנס לשירותי דואר אלקטרוני באנגליה ולגרום לנזקים בקבצים, בכללם קבצים ששייכים לדוכס מאדינבורו (בעלה של המלכה).

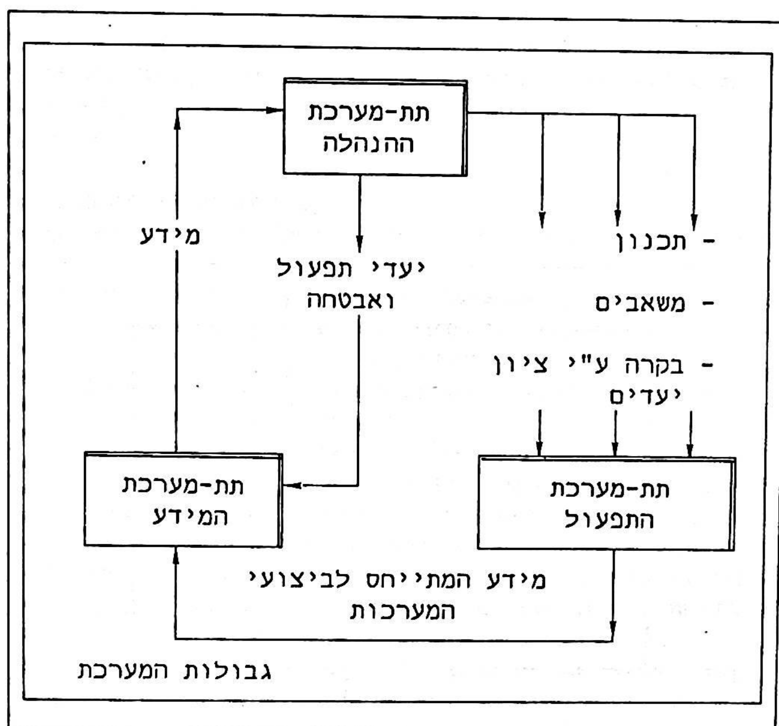
וקיימות דוגמאות רבות נוספות.

אי אפשר להגיע להגנה מושלמת, אך אפשר להגיע לרמות הגנה גבוהות, גם במשאבים מוגבלים. כללית, אפשר לבצע שיפורים משמעותיים באבטחה במחיר זניח, בהשוואה לנזק או לאובדן שעלולים להגרם. ללא קשר לכך יש לציין, שהמחיר הוא גורם חשוב בבחירת אמצעי האבטחה.

1.2 מבוא לאבטחה של מערכות מידע המבוססות על מחשב

אפשר לראות את הארגון כמערכת המאחדת שלוש תת-מערכות: תת-מערכת התפעול, תת-מערכת ההנהלה ותת-מערכת המידע - כפי שמודגם בתרשים 1.1. תת-מערכת התפעול מקיפה את כל המשאבים,

האנשים והפעילויות הקשורים לפונקציות העיקריות של הארגון. תת-מערכת ההנהלה כוללת את כל המשאבים והפעילויות הקשורים לתכנון, לקבלת החלטות ולבקרה של התפעול. המידע, שהוא מרכיב בסיסי בכל ארגון מודרני, מסופק על ידי תת-מערכת המידע, שהיא שילוב של מכונות, פעילויות ואנשים. תת-מערכת זו אוספת ומעבדת מידע, כדי לספק את דרישות המידע של ההנהלה (ראה גם תרשים 1.2).

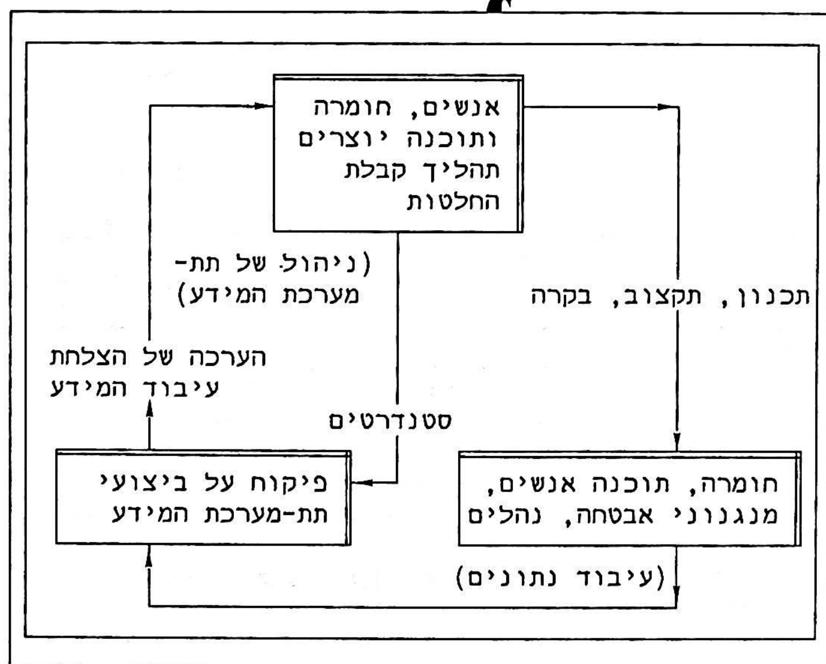


תרשים 1.1 ארגון כמערכת

לתת מערכת המידע חשיבות עליונה לארגון, ויש להתייחס אליה כאל מערכת בפני עצמה. יש לספק את המידע במהירות ובדייקנות. לעתים קרובות ניתן לעשות זאת רק בעזרת מערכות המבוססות על מחשב. מערכות מידע המבוססות על מחשב תמכו בעבר רק בבקרה של פונקציות תפעוליות בסיסיות עם יישומים טיפוסיים, כמו ניהול מלאי, מערך משכורות והנהלת חשבונות. מגוון השימושים במערכות המידע המבוססות על מחשב הורחב בימינו, והוא כולל גם פונקציה של קבלת החלטות, שמתבססת על מערכת תמיכה בהחלטות ועל מערכות

שמבוססות על מאגרי מידע. לכן, הפעילות התקינה של המחשבים ומערכות המידע, הדיוק והאמינות של הנתונים, הם מרכיב בסיסי בפעילות השוטפת של הארגון.

בעולם לא מושלם כשלנו, קשה לצפות שלמערכות המידע לא תהיינה נקודות תורפה. הן יכולות להופיע בצורות שונות, כמו למשל, בחשיפה לא מורשית של מידע סודי ורגיש, בסיכון לבטחון לאומי, או באובדן כספי. אמצעי האבטחה חיוניים לארגונים שמעוניינים בהקטנת הסכנות והאיומים ככל האפשר. לצערנו, מידת הרגישות של מערכות המידע שונה בכל מערכת ושונים גם הסיכונים שמאיימים עליה. לכן לא ניתן ליצור "מתכון" כללי של אמצעי אבטחה שינטרלו כל איום, אלא יש להתאים את אמצעי ההגנה לכל מערכת מידע בנפרד.



תרשים 1.2 מרכיבי תת-מערכת המידע

1.3 פגיעות באבטחה

דוחות רבים מתארים מקרים של ניצול לרעה של מערכות מידע המבוססות על מחשב (ראה פרק 11). ניצול לרעה מקבל, בין היתר, את הצורות הבאות:

* גניבת משאבי מחשב.
* גניבת משאבי החברה בעזרת מערכת המידע.
* גישה לא חוקית לנתונים, או שימוש לא חוקי בהם.
* גניבה של תוכנה מוגנת.

נתייחס לאירועים אלה כפגיעות באבטחה. בטבלה 1.1 תמצא רשימה של אירועים כאלה ותיאור הנזק שהם גורמים. נזק זה מתבטא, במקרים רבים, בירידת רמת השירות של מערכת המידע, שבאה לידי ביטוי על ידי:

(1) אובדן זמינות שירותי המידע (שירות אינו ניתן בזמן הדרוש).
(2) אובדן השלימות (המערכת עושה משהו שלא היה עליה לעשות, או שאינה עושה דבר שהיה עליה לעשות; או שערכי הנתונים שגויים).
(3) אובדן הסודיות (נתונים נחשפים לאנשים לא מורשים).

זמינות ושלימות מתייחסות לכל מערכות המידע, אך סודיות אינה מתייחסת לכולן. על אבטחה של מערכות מידע לשאוף להסיר, או להקטין, את הסיכונים לשירותי המחשוב. אבטחת מידע היא מקצוע בין תחומי והיא עוסקת בחומרה, מערכת הפעלה, יישומים, אנשים וארגונים. אפשר שחשיבות האבטחה חורגת מהממד הטכני שלה, והיא כוללת גם את מדעי ההתנהגות והחברה (פרקר, 1981). התנהגות בני האדם היא נושא מרכזי באבטחה.

1.4 איומים, אמצעי-נגד ופונקציות אבטחה

פגיעה באבטחה יכולה להגרם על ידי:
(1) פעולות בשגגה
(2) פעולות במכוון

לדוגמה, שריפה יכולה להגרם על ידי קצר חשמלי, שהוא פעולה לא מכוונת, או על ידי הצתה, שהיא פעולה מכוונת. מתכנן טוב ינסה לזהות איומים כאלה לפני שיתממשו, כדי שיוכל לתכנן את אמצעי הנגד שיש לשלב במערכת המידע.

טבלה 1.1 איומים, פרצות ואמצעי-נגד

איום	אובדן	פרצה באבטחה	אמצעי נגד
אש	זמינות שירותי מחשב	הרס של נתונים וחומרה	גלאי אש ועשן
הכנסת נתונים מזויפים	שלימות	תרמית פיננסית ושיבוש נתונים בקובץ	נוהלי הכנסת נתונים ובקרות מנהליות
עיון ללא הרשאה בדוחות מחשב	סודיות	גישה ללא הרשאה לנתונים רגישים	בקרות מנהליות
עיון במסוף ללא הרשאה	סודיות	גישה ללא הרשאה לנתונים רגישים	בקרת כניסה למסוף
תקלה במסוף מחשב	זמינות	הפרעה לשירותי המחשוב	מסוף גיבוי (נוסף)
רעש המשפיע על שידור הנתונים בתקשורת	שלימות וזמינות	אובדן נתונים	מספור רץ של הודעות
גניבת קובץ נתונים על ידי עובדי המחשב	זמינות	נתוני החברה לא זמינים	בדיקות מקדימות של העובדים ונוהלי תפעול טובים

בטבלה 1.1 מובאות דוגמאות של איומים, פרצות באבטחה ואמצעי נגד. שלבי התכנון המורכבים של אמצעי הנגד לאיום מסוים, מתוארים בפרקים 2, 3, 4 ו-8, אך ניתן לומר בהכללה שזהו הנושא של כל פרק בספר. לדוגמה, האיום של גניבת תוכנה מוגנת והאמצעים הננקטים נגדה, כמו חוק זכויות יוצרים וחוק הפטנטים, מתוארים בפרק 10 ובנספח החוק הישראלי. בכל שלבי התכנון, חייב המתכנן לבחון את אמצעי הנגד ביחס לפונקציות שהן אמורות למלא:

(1) מניעה - (prevention) הגישה התיאורטית האידיאלית, שניתן להגשימה לעתים רחוקות בלבד, בגלל עלות הבנייה והתפעול של אמצעי הנגד.

(2) גילוי - (detection) לעתים קרובות ניתן לשלב את אמצעי הגילוי והמניעה. לדוגמה, בתהליך הזיהוי והאימות, המתואר בתרשים 3.1, נמנעת כניסה ללא הרשאה ובנוסף לכך, נרשמים כל ניסיונות הכניסה הכושלים, כדי לאתר פעילות לא חוקית.

(3) הרתעה - (deterrence) לעתים קרובות כדאי לגרום לכך שפושעים פוטנציאליים יהיו מודעים לקיומם של אמצעי גילוי ונוהלי אבטחה אחרים, כי הפחד להתגלות עשוי למנוע פשע.

(4) אישוש - (recovery) במצבים בהם מניעה, גילוי והרתעה אינם יעילים בהתמודדות עם איום, נדרשים נוהלי התאוששות, כמו: נקודות ביקורת בעבודות שזמן העיבוד שלהן ארוך, או קבצי גיבוי.

(5) תיקון - (correction) לאחר ההתאוששות ממצב התקלה, יש לתקן מיד את הגורמים שגרמו לתקלה.

(6) מניעה - (avoidance) כאשר אמצעי הנגד אינם מספקים, הדרך היחידה להמשיך ולפעול היא שנוי התכנון, כדי להסיר לחלוטין את האיום.

כללית, "תאונות", או תקלות, שנגרמות מטעויות אנוש גורמות לאובדן גדול יותר מפגיעות מכוונות. לכן, יש להשמר בראש ובראשונה מ"תאונות" כאלה. חשוב לציין: מערכת שיכולה לספוג מספר רב של טעויות פותחת אפשרויות רבות לפעילות בלתי חוקית המוסתרת על ידי טעויות. אמצעי נגד המפחיתים את ספיגת הטעויות, תורמים להקטנת הסיכון מפני פעילות מכוונת, שמטרתה לנצל לרעה את המערכת.

1.5 רגישות של יישומים

מערכות מידע פגיעות מגוון רחב של סיכונים (FIPS 65, 1979). יש צורך להעריך את הפגיעויות (vulnerabilities) האלו, כדי להבין את הבעיות שאנו דנים בהן בספר זה. בטבלה 1.2 מובאות מספר דוגמאות של פגיעות וניתן לראות שהן פרושות ממצב של קלט נתונים ועד לטעויות במערכת ההפעלה.

בשלב תכנון אמצעי ההגנה, יש לזהות את חולשותיו של כל יישום בנפרד, אך אין די בכך לבחירת אמצעי ההגנה. יש להתחשב גם ברגישות של היישום (FIPS 73, 1980). מידת הרגישות של מערכת מידע תלויה בנתונים שהיא מעבדת ובדרך שבה המערכת תומכת בשירותים עסקיים אחרים. לדוגמה, רשומות של תשלומים וחובות בחברת מימון הן הרגישות ביותר. דוגמאות של מערכות שעלולות להיות רגישות מובאות בטבלה 1.3. על כל ארגון לבחון את היישומים שלו בכדי לקבוע את מידת רגישותם.

טבלה 1.2 פגיעויות של נתונים במערכות מידע

תחום הפגיעה	דוגמאות	סוג האיום
קלט	ניתן לשנות נתונים, לאבד אותם, או לקרוא אותם באופן שגוי.	מכוון לא מכוון מכוון
גישה	אין בקרה על משתמשי המערכת, ועל המחזיקים בגישה לנתונים. הכניסה אינה נרשמת ולכן, הנתונים חשופים גם לאנשים לא רצויים.	מכוון מכוון
נתונים לא מוגנים	נתונים בקבצים מקוונים חשופים לגישה לא מורשית. ניתן לגשת לקבצים בספריות בקלות ובאופן לא רשמי.	מכוון מכוון
טעויות בתכניות	טעויות חישוב. תכניות סמויות (סוס טרויאני, או וירוס, למשל) שמשולבות בתכניות אמיתיות, יכולות להעתיק נתונים לקבצים אחרים לשימוש בשלב מאוחר יותר.	לא מכוון מכוון
מערכת ההפעלה	טעויות בתכנון ו/או בהתקנה מאפשרות למשתמש לעקוף את הבקרות, למחוק את נתיבי הביקורת ולהכנס לכל קובץ.	מכוון
בקרות בתוכנה יישומית	בקרות במערכת פיננסית יכולות להיות חלשות ולאפשר למשתמש: 1. להכניס נתונים מזויפים כדי לבצע מעשה מרמה. 2. להכניס נתונים שגויים שיכולים לפגוע בשלימות הנתונים.	מכוון מכוון

1.6 הגדרות

עד כאן הצגנו כמה מונחים באבטחה. בסעיף זה מקובצים החשובים שבהם, שמוגדרים בהתאם למינוחי מכון התקנים האמריקאי (NBS), בפרסום FIPS 73, 1980. בפרקים הבאים יוצגו ויוגדרו מונחים נוספים.

שלימות - שלימות נתונים קיימת כאשר הנתונים במחשב זהים לאלה שבמסמכי המקור ולא ניתן לשנות (במכוון או בשגגה), להרוס או לחשוף אותם. שלימות מערכת פירושה שהמערכת פועלת בהתאם למפרט של המתכנן והיא עמידה בפני ניסיונות לשבש אותה. שלימות היא המפתח לדיוק ואמינות.

זמינות של שירותים - מצב שבו מערכת המידע מספקת שירותים ברצף ובפרקי זמן קצובים.

סודיות - תפיסה המיושמת עבור נתונים שחייבים להיות סודיים ומוגנים בפני חשיפה ללא הרשאה.

פרטיות - תפיסה שמיושמת לפרט. הזכות של כל אדם לקבוע איזה חלק מהמידע שמתייחס אליו מותר לעיון על ידי אחרים.

פגיעות - נקודה חלשה במערכת המידע, המאפשרת לנצל לרעה את המערכת ולהעמיד בסכנה את המידע ואת השירותים שהיא מספקת.

איום - איום הנוצר על ידי אדם או אירוע, ומהווה סכנה פוטנציאלית למרכיב של מערכת המידע. התוצאה של האיום יכולה לשבש את פעולת המערכת, על ידי שינוי או פגיעה במטרות פעולתה.

אובדן - התוצאה הסופית והלא רצויה של איום. למשל, ההוצאה הכספית הנוספת, או הנזק האפשרי, במקרה של אובדן שירותים. יחסי הגומלין בין אובדן לפגיעות ובין איום לפגיעות מתוארים בתרשים 1.3.

סיכון - הערכה כמותית של אובדן.

הגנה - אמצעי להגנה מפני אובדן.

אבטחה - הגנה על נתונים בפני איום מכוון או לא מכוון, שיכול לגרום לשינוי, חשיפה או הרס של נתונים ללא הרשאה; שמירה על פעולתן התקינה של מערכות המידע מפני ירידה ברמת השירות או הפסקת השירות לחלוטין.

טבלה 1.3 יישומים שעלולים להיות רגישים

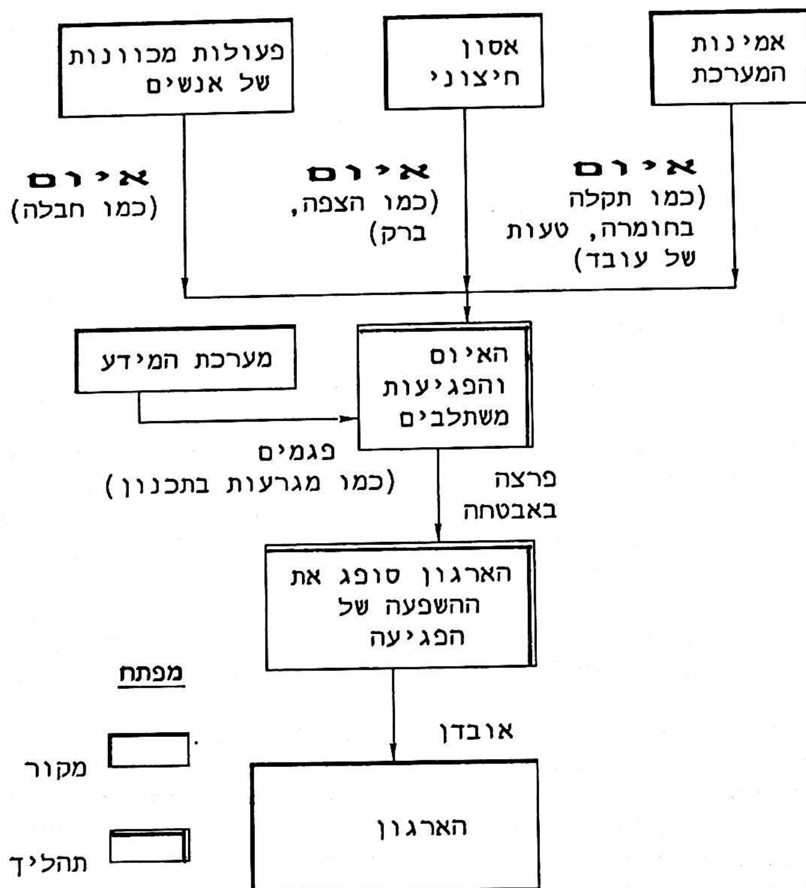
סוג היישום	דוגמאות	יעדי האבטחה
1. הנהלת חשבונות	1.1 הנה"ח של קניות 1.2 הנה"ח של מכירות 1.3 משכורות 1.4 ניהול מלאי	שמירה על שלימות הנתונים
2. תכניות מחשב כלליות	2.1 לו"ז של תחזוקת המתקן 2.2 הדמייה של רשת לחלוקת מים 2.3 תיב"מ	שלימות נתונים
3. קבלת החלטות אוטומטית	3.1 הזמנת פריטים למלאי 3.2 תשלומים אוטומטיים	ביקורת קפדנית על שלימות הנתונים
4. מידע להנהלה	4.1 ניהול מרכזי של יחידת המחשב 4.2 בסיסי נתונים מרכזיים	שמירה על סודיות המחשב ושלימות הנתונים
5. בקרה בזמן אמת	5.1 בקרת רמזורים 5.2 בקרה אווירית 5.3 פיקוח אוטומטי ברצפת הייצור	שמירה על פעולה שוטפת ותקינה של המחשב וביקורת קפדנית על שלימות הנתונים
6. מערכות ציבוריות ולאומיות	6.1 העברת כספים אלקטרונית (EFT) 6.2 בקרה של חומרים גרעיניים 6.3 בטחון לאומי 6.4 עיצוב חדש של מכונית אצל יצרן מכוניות	שמירה על סודיות ושלימות הנתונים עם יכולת עיבוד שוטפת

1.7 סיכום

מערכות מידע המבוססות על מחשב חיוניות לתפעול יעיל של ארגון מודרני. קשה לתת הערכה כמותית לערכו של המידע, אך במקרים רבים מחזיקים ארגונים במידע ייחודי שההרס שלו עלול לגרום לשיתוקם. לכן יש לאבטחה חשיבות עליונה. הצורך באבטחה בולט ביותר במערכות פיננסיות, אך הוא גורם בסיסי בכל המערכות העסקיות, מוסדות ציבוריים, מתקני צבא ובטחון, מכוני מחקר ועוד. האבטחה תהיה מושלמת רק אם נתחשב, בנוסף למימד הטכני, גם במימדים אחרים, כמו ההיבט הפסיכולוגי והסוציולוגי של התנהגות האדם. אבטחה של מערכות מידע המבוססות על מחשב מטפלת בנוהלים ובאמצעים טכניים שמיושמים בתוכנת היישומים, במערכת ההפעלה, בחומרה, באנשים, בארגון ובנתונים. מטרת אמצעי ההגנה לסוגיהם היא להגן על הנתונים שבמערכת המידע בפני חשיפה, או גישה ללא הרשאה.

האבטחה היא חלק אינטגרלי בתכנון, בהתקנה ובתפעול של מערכת המידע. כללית, שיפור האבטחה ייתכן רק אם הארגון יטפל בכל מערכת בנפרד. יוצאות מכלל זה מערכות הנוגעות לבטחון לאומי (FIPS 73,1980). במקרה מיוחד זה, קיימת סכנה שנקודות התורפה בתוכנות המערכת ינוצלו לרעה, כדי לעקוף את הבקרות שנבנו בתוכנות היישומים. לכן, יש לשלב תחילה את האבטחה במערכת ההפעלה ורק לאחר מכן לתכנן את היישומים. ספר זה מטפל באבטחה של מערכות מידע בסביבה עסקית רגילה.

אבטחה עולה בכסף ולכן יש לאזן את עלות הרכישה, ההתקנה והתפעול של אמצעי ההגנה עם התועלת שתופק מהם. המאזן לא יהיה תמיד לטובת האבטחה, אך תהיה זו טעות להתעלם לחלוטין מצורכי האבטחה. לצערנו, לעתים קרובות מתעלמים מצורכי האבטחה, מכיוון שזו בעיה חדשה באופן יחסי למנתחי מערכות ולמנהלים. כמו כן, האסונות נדירים יחסית ולעתים אין שומעים אודותיהם. תוכנית אבטחה מדוקדקת תביא לניצול יעיל של המשאבים. תוכנית כזו תמנע מאיומים רבים להתפתח לפרצות באבטחה, ואם תתרחש פרצה כזו, תספק תוכנית האבטחה בסיס להתאוששות מהירה.



תרשים 1.3 יחסי הגומלין בין איומים, מגרעות, פרצות ואובדנים

טבלה 1.4 סקירה של בקרות המשמשות באבטחה

מנגנוני בקרה חיצוניים	בקרות במישק משתמש-מחשב	בקרות פנימיות במחשב
ניפוי וסיווג כ"א	אימות משתמש	בקרת כניסה
הגבלת הכניסה לחדר המחשב	ניהול סיסמאות	בקרת זרימה
הגבלת הכניסה לחדרים המכילים מסופי מחשב	ניטור אמצעי האבטחה	בקרת היקש לוגי - (Interference Control)
הגנה בפני אש	ביקורת ענ"א	בקרת מידע במעבר, תוך שימוש בהצפנה
הגנה בפני הרס		
הגנה בפני גניבה של אמצעי אחסון נתיקים		

שאלות

1.1 הסבר את המונחים: איום, מגרעות תכנון, פרצה ואובדן.

1.2 הסבר את המונחים: שלימות, סודיות, אבטחה ופרטיות.

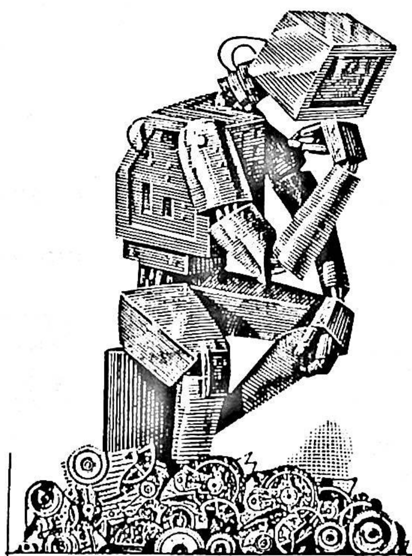
1.3 מאפייני האבטחה של מערכת חדשה צריכים להיות פתוחים להליכי בדיקה וביקורת קפדניים. הסבר מהם היתרונות והחסרונות שבגישה זו.

1.4 אחד מעובדי החברה אינו מורשה להשתמש במשאבי המחשב שלה, למרות שיש לו ניסיון בשימוש במחשבים מעבודתו הקודמת. בוקר אחד, כאשר היה פנוי, מצא עובד זה במחלקה אחרת מסוף שלא היה בשימוש. ליד המסוף היה מונח תדפיס ששייך למשתמש קודם, שמתוכו אפשר היה ללמוד את פרוטוקול הגישה (login), את שם המשתמש, את מספר החשבון, אך לא את הסיסמה. הפורץ החליט לנסות לחדור למחשב על ידי ניחוש

הסיסמה. לאחר 60 ניסיונות, הצליח הפורץ להכנס וקיבל את מלוא ההרשאות. הוא עבד על המסוף כשעה, ואז הלך לאכול ארוחת צהריים. אחר הצהריים חזר הפורץ ומצא שאין צורך בכניסה חוזרת למחשב, מכיוון שהמחשב לא ניתק את המסוף. הוא ביצע כמה שאילתות נוספות ולאחר שעה ניתק את הקשר (log off), אסף את הניירות שלו ועזב.
הסבר את נקודות התורפה באבטחה, לפי המקרה שתואר, והצע תוכנית לשיפורים.

1.5 זהה סוגים של עובדים בארגון שלך שיכולים להיות מעורבים בפגיעה מכוונת במתקני המחשב ומערכות המידע. נסה למצוא סיבות להתנהגותם.

1.6 מהו ההבדל בין צורכי האבטחה של מערכות מידע המבוססות על מחשב, לבין צורכי האבטחה של מערכות ידניות המשתמשות בפקידים ובארונות תיקים?



חשוב ותכנן!

פרק 2

אבטחה פיסית של חדר המחשב

אבטחה פיסית היא חלק חיוני מכל תוכנית אבטחה. היא משלימה את מאפייני האבטחה המסופקים על ידי החומרה, התוכנה והבקרות המנהליות. לאבטחה פיסית פנים רבות, כמו הגנה בפני אש, חומרי הבנייה ובקרת הכניסה, שאפשר לקבצן בשתי קבוצות:

1. הגנה בפני אסונות טבע, כמו הצפה ואש.
2. הגנה בפני מסיגי גבול לסוגיהם.

2.1 אסונות טבע ומסיגי גבול

אבטחה פיסית מתייחסת לבקרות ומנגנונים בתוך מרכז המחשב וסביבו ולמתקנים מרוחקים שקשורים אליו. בקרות ומנגנונים אלה מיועדים להגן על החומרה ועל אמצעי האחסון הנתיקים של הנתונים. כפי שאפשר לראות בטבלה 2.1, קיים מגוון רחב של איומים על מתקן המחשב מצד הסביבה הפיסית שבה הוא נתון. לסביבה הפיסית משקל רב באבטחה של מערכות מידע ולכן, חיוני להקדיש מחשבה לגורמים כמו מיקום הבניין, תכנונו ומבנהו. יש לעשות זאת מוקדם ככל האפשר בתהליך התכנון של מתקן המחשב, מכיוון שבשלב זה קל עדיין להתגבר על בעיות האבטחה.

2.2 אסונות טבע

מזג האוויר הינו האיום הטבעי הגדול ביותר לרוב המתקנים, אך רק מתקנים מעטים מחוסנים ממצבים קיצוניים של מזג האוויר. לרוח, לגשם ולסערות עלולות להיות השפעות דרמטיות. לדוגמה, ברק לא יכול לגרום נזק לבניינים מודרניים שמוגנים בצורה נכונה, אבל הוא עלול לגרום להפסקה באספקת זרם החשמל וכתוצאה מכך - להשפיע על שירותי המחשוב. הצפה מגגות דולפים למשל, עלולה לפגוע במידה שווה, אך האיום הגדול ביותר למתקני המחשב הוא האש.

טבלה 2.1 איומים

מקור	דוגמאות	סוג האיום
אסונות טבע	אש, סערה, ברקים, הצפה	לא מכוון
מעשה ידי אדם	חוסר כישרון, סקרנות, הפרות סדר חיצוניות, טעויות אנוש	לא מכוון
מעשה ידי אדם	חבלה מבפנים חבלה מבחוץ	מכוון

הסביבה הארגונית היא זו שיוצרת את המערכת הספציפית של הפגיעויות למתקן מסוים. כפי שאפשר לראות בטבלה 2.2, קיימים גורמים רבים שעלולים להגדיל את סיכוני הפגיעה.

טבלה 2.2 גורמים המגדילים את סיכוני הפגיעה

1. מרכז מחשב הפתוח לעובדים ממחלקות רבות בחברה ולאנשים מארגונים אחרים.
2. ריכוז של משאבי מרכז המחשבים באתר אחד.
3. מרכז מחשבים הממוקם בסביבה בעלת רמת סיכון גבוהה. לדוגמה: באיזור מועד לשטפונות, במקום הקרוב למתקן כימי או למתקן המכיל חומרים דליקים, או בסביבה בעלת רמת פשיעה גבוהה.
4. תחלופה גבוהה של עובדים.
5. רמת מוסר נמוכה של עובדים.

2.2.1 סיכוני אש וההשפעה של בחירת האתר

סרטים מגנטיים, דיסקטים ופלט מחשב רגישים לאש. אם הם נפגעים ונגרם להם נזק, אי אפשר לשחזר את המידע שהיה מוקלט בהם. כספות חסינות אש יכולות להגן על אמצעי האחסון המגנטיים ואף על מסמכים חשובים. כדי להתגבר על בעיות אש כלליות, יש לנקוט בכמה אמצעי זהירות, שתפקידם:

(1) למנוע התלקחות אש.
(2) לגלות קיומה של שריפה קרוב ככל האפשר לזמן ההתלקחות.
(3) תיקון המצב בנזקים פחותים ככל האפשר.

תוכנית לבטיחות אש כוללת את הסעיפים הבאים:

* בחירת האתר והכנתו.
* גילוי אש.
* כיבוי אש.
* התאוששות.
* פינוי אנשים מהאתר.

טבלה 2.3 מכילה רשימה של אמצעי הגנה שיינקטו בהפעלת של תוכנית הגנה מתאימה.

טבלה 2.3 אמצעי הגנה בפני אש

פונקציית ההגנה	דוגמאות
(1) מניעה	חומרי הבנייה של המבנים. נוהלים למניעת אש (כמו בקרה על אחסון חומרים דליקים).
(2) גילוי	גלאי חום ועשן (שיכולים להפעיל את אמצעי הכיבוי).
(3) כיבוי	מערכות להתזת מים (sprinkler systems). מערכות להתזת גז במקומות שבהם יש ציוד חשמלי (Halon הינו יקר, אך בכמויות קטנות הוא אינו מזיק לאנשים, שלא כמו CO_2, שגורם נזק). הדרכה ואימון של כל העובדים בהתגוננות בפני אש וקביעת אחראים לנושא בכל מחלקה. שלטים ברורים המורים על היציאות של הבניין ועל מיקום הציוד לכיבוי אש.

בבחירת האתר ובהכנתו יש להתייחס לגורמים הבאים:

(1) **בדיקת קירבה** - בדיקה של כל המבנים והשטחים הקרובים לאיזור המחשב, כדי לבדוק אם נמצאים באיזור גורמים בעלי רמת סיכון גבוהה, כמו מחסני נייר, חומרים דליקים, או תהליך כימי מסוכן.

(2) **בדיקה של מאפייני הבנייה וחומרי הבנייה** - אם הם רגישים פחות לאש. יש לשים לב למאפייני תיכנון, כמו קיר חוצץ אש העוזר לבלום את האש, שימוש בחומרי בנייה שרגישים פחות לאש.

2.2.2 גילוי אש

אש מתפתחת בשלושה שלבים, כפי שאפשר לראות בטבלה 2.4. בתחילה ישנה בעירה איטית; לאחר מכן האש מתפשטת בעזרת מגע ישיר; ולבסוף האש מספיק חזקה כדי להתפשט בעזרת חום וקרינה. גלאי חום יכולים לגלות את האש בשלב האחרון, שבו כבר קשה לשלוט בה. לכן, יש להשתמש בגלאי עשן, כדי לנסות לאתר את האש לפני שהיא יוצאת מכלל שליטה. כדי למנוע את התפשטות האש במגע ישיר, יש לבודד מחסנים עם חומרים דליקים ולהתקין בהם גלאי אש ועשן.

גלאי עשן פועלים על פי שני עקרונות:

(1) עיקרון הפיזור האופטי - מגלה עשן בעזרת האור שמתפזר בשעת הפגיעה בחלקיקי העשן. ציוד הפועל לפי עיקרון זה, יגלה גם עשן לבן בריכוז המופק על ידי בעירה של כבל המצופה PVC.

(2) עיקרון תא היוניזציה - ציוד הפועל לפי עיקרון זה אינו רגיש לעשן הנפלט מבעירה של PVC, אבל הוא יגלה אש בפח אשפה ביתי לפני שהעשן יופיע.

גילוי אפקטיבי דורש שילוב של גלאי חום וגלאי עשן. בין גלאי העשן יש לשלב בין אלה הפועלים לפי עיקרון הפיזור האופטי לבין אלה הפועלים לפי עיקרון תא היוניזציה.

טבלה 2.4 התפתחות האש, סימנים ואמצעי גילוי

השלב	הסימן	אמצעי הגילוי
(1) מייד לאחר ההצתה	עשן	גלאי עשן
(2) התפשטות האש דרך מגע ישיר	עשן	גלאי חום
(3) התפשטות האש דרך קרינת חום	עשן וחום	גלאי חום

2.2.3 כיבוי אש

לאחר שהאש יוצאת מכלל שליטה, אפשר לכבות אותה בעזרת האמצעים הבאים:

(1) מטפי יד
(2) זרנוקים
(3) מטפי גז אוטומטיים
(4) מערכת התזה אוטומטית (sprinkler system)

מטפי יד נפוצים ברוב המבנים, אבל במקרי חירום מעטים בלבד יודעים להפעילם. בניגוד לזרנוקים, לא נדרשת מיומנות רבה להפעלת מטפי יד, אבל חשוב שתתבצע הדרכה, כדי להקנות לעובדים מיומנות בשימוש בהם. מומלץ שרק צוות כיבוי אש מקצועי ישתמש בזרנוקים (ראה טבלה 2.5).

טבלה 2.5 רמת המיומנות הנדרשת כדי לתפעל ציוד לכיבוי אש

הציוד	המפעיל
מטפי יד	כל אדם שקיבל הדרכה בסיסית
זרנוקים	מקצוענים
מערכות התזה אוטומטיות	אוטומטי
מטפי גז אוטומטיים	אוטומטי

קיימים שני סוגים של מטפי גז אוטומטיים: האחד פועל בעזרת CO_2 והשני - ב-Halon. מערכת לפיזור מכבה את האש על ידי הצפת חדר המחשב בגז. הגז יכול להגיע לכל מקום ולכן, מטפי גז אוטומטיים יעילים במיוחד במקומות סגורים, כמו קומת ביניים, שאליהן קשה להגיע בשיטות אחרות. יתרונם של CO_2 ו-Halon הוא בכך שאינם גורמים נזק למחשב ולציוד ההיקפי. לצערנו, CO_2 גורם נזק לבני אדם, כי במהלך כיבוי האש, הוא תופס את מקומו של החמצן. כדי לכבות אש בפח אשפה קטן נדרשת כמות של גז השווה ל-30% מנפח החדר שבו נמצא הפח, ויש לזכות שדי בריכוז של 10% כדי לגרום לאובדן הכרה. לכן, אין להשתמש ב-CO_2 כאשר נמצאים אנשים במבנה ומותר להעביר את המערכת למצב פעולה אוטומטי רק לאחר פינוי המבנה מיושביו. כמו כן, CO_2 אינו יכול להתמודד עם אש הניצתת מחדש לאחר שהגז הוזרם. עם זאת, CO_2 מספק הגנה מצוינת, מכיוון שהוא זול ויעיל מאוד, אך בהתקנות חדשות לא מומלץ להשתמש בו, בגלל הנזק שהוא עלול לגרום לבני אדם.

Halon אינו כה מסוכן לבני אדם, מכיוון שאין הוא תופש את מקומו של החמצן במהלך כיבוי האש. הוא פועל על השריפה בצורה כימית. Halon יקר יותר מ-CO_2, אך נדרש ממנו ריכוז נמוך יותר כדי לעצור את תהליך השריפה (האסיאו, 1979). ללא קשר לגז שבו הוחלט להשתמש, יש לקבוע שלטי אזהרה מתאימים בכל הכניסות לשטח המוגן. מותר להעביר את המערכת למצב אוטומטי רק בזמן שאין אנשים בבניין.

מערכות להתזת מים טובות לכיבוי שריפות של מוצרי נייר ובנייה, אך לא לשריפות של ציוד חשמלי. מערכת להתזת מים טיפוסית מתבססת על צינורות המשחררים מים בלחץ לאחר ששסתום התזה מופעל בבניין. שסתום זה מופעל בטמפרטורה של $80^{\circ}C$, כאשר השריפה במצב מתקדם וכבר נגרם נזק כבד. יש לזכור שמטרתן העיקרית של המערכות להתזת מים היא למנוע נזק כבד, שפירושו - הרס כללי.

בטבלה 2.6 נערכת השוואת יעילות השימוש בין מטפי גז הלון לבין מערכות להתזת מים.

טבלה 2.6 השוואה בין מטפי גז Helon לבין מערכות להתזת מים

המאפיין	מטפי גז Halon	מערכות להתזת מים
יעילות	גבוהה מאוד	גבוהה מאוד
השפעות לוואי	מעטות	נזק אפשרי לציוד
התאוששות	שעות	דקות, אם אספקת המים עדיין פועלת
הוצאות תפעול	גבוהות	לא משמעותיות

2.2.4 סיכוני טבע אחרים

הסיכון המשמעותי הבא למחשבים, אחר האש, הוא המים, כתוצר לוואי של כיבוי אש או כתוצאה מהצפה. אם חדר המחשב ממוקם במקום שעלול לסבול מהצפות, יש לשקול שימוש באמצעים שיבטיחו הגנה ממים. הצפה יכולה להיגרם משטפון, אך מקורן של רוב ההצפות הוא נזילות מהתקרה, שעלולות להתרחש אם התקרה איננה

אטומה מספיק. הצפות עלולות להגרם גם משינויים אקלימיים, או מפגיעה במערכת הניקוז של הגג, או של קומות עליונות.

יש לדאוג לאספקה סדירה של שירותים, כמו מים וחשמל, ולהבטיח שאספקת הכוח תהיה אמינה, כי מרכזי המחשבים הם צרכנים כבדים של חשמל. מומלץ להשתמש גם ביחידות UPS ובמקור מתח חלופי, כדי להבטיח את אספקת הזרם במקרים של תקלות ברשת הציבורית. יש לזכור שניתוק פתאומי של מחשב מזרם החשמל בעודו פועל, עלול לגרום לנזקים כבדים, הן ליישומים והן לחומרה.

2.3 בקרת כניסה ומסיגי גבול

היעד הבסיסי של בקרת הכניסה הוא לאפשר כניסה רק לאנשים המחזיקים בהרשאה להיות בשטח המוגן ולדחות את כל אלה שאין להם אישור להיות בו. אם נקטין ככל האפשר את מספר המחזיקים באישורי כניסה לאיזור רגיש כמו המחשב, נערים קשיים רבים בפני פורץ פוטנציאלי וסביר להניח שהוא יתגלה, אם יעלה בידו להכנס לשטח.

על תוכנית הגנה להכיל את הנושאים הבאים:

(1) הגדרה של שטחים פיסיים שהכניסה אליהם תהיה מבוקרת.
(2) הרשאות כניסה לכל שטח מבוקר, לכל סוג של עובדים ולאנשים מארגונים אחרים.
(3) סוגי בקרות הכניסה שייעשה בהן שימוש.

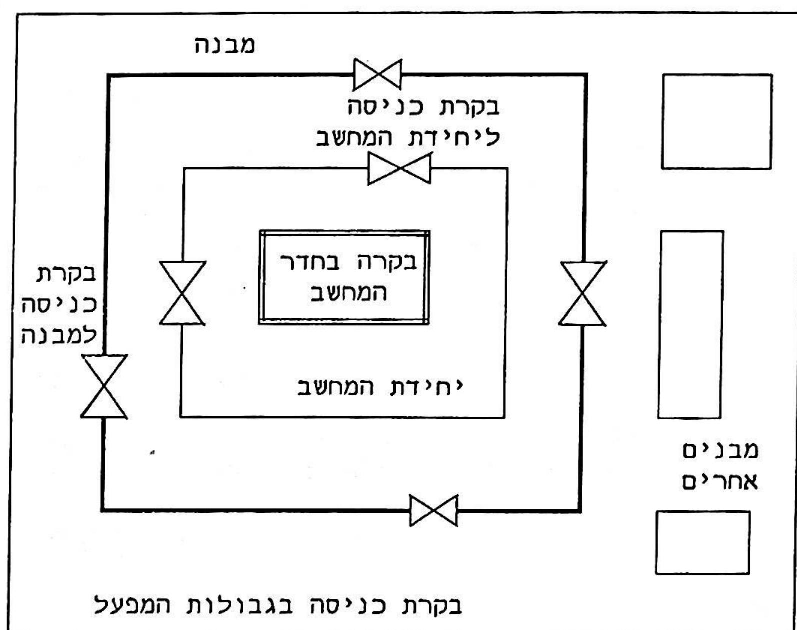
2.3.1 איזורים רגישים

ההגנה של מרכז המחשבים והסביבה הפיסית שלו מחולקת לארבעה חלקים:

(1) הגנה היקפית שמתייחסת לשטח הנמצא מחוץ למבנה ובדרך כלל, עד לגבולות המפעל.
(2) בקרת כניסה למבנה.
(3) בקרת כניסה למחלקת המחשב.
(4) בקרת כניסה לאיזורים רגישים, או למרכז המחשבים עצמו (AFIPS, 1979; הסיאו, 1979).

למרות שאין זה ישים לבנייני משרדים, יש לציין שגדר המקיפה את הבניין או המפעל היא קו ההגנה הראשון והחשוב ביותר. יש לאבטח כל נקודת כניסה אפשרית למבנה הראשי, כולל דלתות ופתחים קטנים אחרים, כמו חלונות ופתחי איוורור. ההגנה על

מחלקת המחשב ועל מרכז המחשבים הכרחית להצלחת תוכנית האבטחה הכללית. לכן יש להשתמש בשילוב של כמה אמצעים, כמו ביקורת של פקיד קבלה, טלוויזיה במעגל סגור, סיורי שומרים, מנעולי צירופים וכרטיסי זיהוי עם תמונות. בכניסה לספריית הסרטים יידרשו אמצעים נוספים, כדי להבטיח שלא יילקחו סרטים ללא רשות.



תרשים 2.1 בקרת כניסה לאיזורים רגישים

2.3.2 אנשים עם צורכי כניסה שונים

לאחר שהארגון קבע את השטחים הרגישים, יש להבטיח שרק האנשים העובדים במקום באופן קבוע יוכלו להכנס בצורה חופשית. התנועה של שאר האנשים לתוך השטח הרגיש תבוקר באופן קפדני.

2.3.3 טכניקות לבקרת כניסה

קיימות שלוש דרכים שבעזרתן אפשר לבקר כניסת אנשים:

(1) שימוש באנשים כמנגנוני בקרה (לדוגמה, פקיד קבלה או קציני בטחון).
(2) אמצעים מכניים, כמו מנעולים ומפתחות.
(3) מערכות אלקטרוניות, כמו מערכות המשתמשות בכרטיסי זיהוי וקוראי כרטיסים.

קצין בטחון הבודק את הנכנסים למבנה, או מונע מזרים להכנס לשטח מוגן, הוא דוגמה לשימוש באנשים כמנגנוני בקרה. פקיד קבלה או קצין בטחון העובדים בדרך זו, חייבים להיות בקיאים בהוראות ובנוהלים שנקבעו לכל מצב, כולל: אישורי כניסה, מניעת כניסה ובקשת עזרה. קצין בטחון או פקיד קבלה הם פתרון אידיאלי כאשר מספר המבקרים קטן באופן יחסי, אך ככל שמספר המבקרים עולה, פוחתת יעילותו של קצין הבטחון. אנשים הינם אמצעים יקרים, שאינם מספיק אמינים לגילוי מבקרים שאינם מחזיקים באישורי כניסה. השימוש היעיל ביותר שאפשר לעשות בבני אדם הוא בפיקוח על פעולתן התקינה של מערכות אחרות.

אפשר להשיג רמה בסיסית של אבטחה בעזרת מנעול פשוט בדלת כניסה. שיטה זו טובה להגבלת הכניסה, אבל אין היא מתאימה לפתחים שבהם עוברים אנשים בתדירות גבוהה. במקרים אלה אפשר להגיע לרמה גבוהה יותר של הגנה בעזרת קורא כרטיסים המשולב במנעול. המנעול נפתח על ידי כרטיס המכיל קוד מכני, אופטי או מגנטי המזהה את המשתמש בו. המערכת ששולטת על פתיחת המנעול, מאחסנת את רשימת מספרי הקוד המורשים. אפשר להשתמש במערכת באופן שיתאפשר כניסה לא רק לפי מספר קוד, אלא גם לפי מספר הדלת, שעה ביום ויום בשבוע. כלומר, ניתן לקבוע שעובד מסוים יוכל להכנס ביום ובשעה מסוימים בדלת מסוימת בלבד.

בקוראי כרטיסים נפוצים שכלולים נוספים. לדוגמה, במצבים שבהם נדרשת רמה גבוהה של אבטחה, אפשר לשלב את קורא הכרטיסים במקשים. כדי לזכות בהרשאת כניסה, יש להכניס את הכרטיס לקורא הכרטיסים ולהקיש מספר מזהה אישי. כניסה בעזרת כרטיס ומספר מזהה פשוטה יותר מאשר מנעול ומפתח, אך גם היא גורמת לאי נוחות לצוות העובדים.

במקום שיש בו כניסות עובדים יומיות רבות לשטח מוגן, הפתרון המוצלח ביותר הוא בקרת כניסה אוטומטית. בשיטה זו ההתקן, המנעול או המחסום, נפתח על ידי אות משודר ממשדר קטן, הנישא על ידי העובד. אם מקור המתח למשדר הוא פנימי, עלול המשדר שלו להיות בגודל של מכשיר איתורית הנושא בתוכו מצבר, שאינו

נוח לשימוש. מקור המתח יכול להיות גם חיצוני, ואז המיקרו-מעבד מקבל את המתח שהוא צורך משדה אלקטרומגנטי שיוצר החיישן שמקבל את האות. משדר כזה הוא בגודל של כרטיס מגנטי רגיל ואשר אטום לחלוטין ונוח יותר לשימוש.

כאשר עובד מתקרב לאיזור המוגן, השדה האלקטרו-מגנטי שיוצר החיישן מפעיל את המיקרו-מעבד שבכרטיס וזה משדר באופן אוטומטי את קוד העובד שנקלט על ידי החיישן. המערכת מאמתת שלעובד יש הרשאת כניסה לאותו איזור והדלת נפתחת מייד. בשיטה זו אין העובד צריך להמתין ושיתוף הפעולה מצידו מינימאלי. כרטיסים מסוג זה מוכרים בשם כרטיסי קרבה אשר שימושיים מאוד במקומות שבהם עובדים נכנסים ויוצאים פעמים רבות. במערכות רבות משולב מחשב אישי, שמאפשר ליישם תוכנית בקרת כניסה מורכבת.

בשנים האחרונות מתפשט השימוש במערכות בקרת כניסה המבוססות על שיטות ביומטריות. במערכות אלו אישור הכניסה ניתן לאחר שנעשה אימות לגבי תכונה ייחודית מסוימת של המבקש, כמו גיאומטריה של היד, טביעת אצבעות, חתימה, צורת העין וצבע האישון, קול ועוד. תהליך הכניסה יכול להיות משולב עם כרטיס מגנטי ומקשים ויכול לעמוד בפני עצמו. מערכות אלו נחשבות לאמינות שבין מערכות בקרת הכניסה, אך מחירן עדיין גבוה. לכן מומלץ להשתמש בהן רק באיזורים רגישים במיוחד.

ללא תלות בשיטה שתבחר, הצלחתה תלויה בשיתוף הפעולה של העובדים. באחריות ההנהלה לדאוג שהעובדים ידעו על הסיבות להכנסת מערכת לבקרת כניסה ויבינו מה מצופה מהם לעשות, כדי שתוכנית בקרת הכניסה אכן תצליח.

2.4 מסקנות

כדי לפתח תוכנית מעשית לאבטחה פיסית, יש לנקוט בגישה שיטתית. ההנהלה צריכה להעריך במדויק מה עומדים למנוע ועל מה רוצים להגן, לפני שתבחר באמצעים לאבטחה פיסית. כך יובטח שימוש אופטימלי במשאבים הכספיים. כדי להגיע ליעד זה על הארגון לבצע את הפעולות הבאות:

* לזהות את הסיכונים.
* להעריך את האיומים הפיסיים שעלולים להגרם למחשב ולמתקנים על ידי כל אחד מהסיכונים, ואת הסיכוי להתרחשותם.
* להעריך באופן כמותי אובדנים שעלולים להגרם כתוצאה מהתממשות האיומים.
* להעריך נזק שנתי צפוי.

ניתוח זה נקרא **"ניתוח סיכונים"** (risk analysis) והוא מתואר בפירוט בפרק 8. ניתוח סיכונים מספק להנהלה תמונה כמותית שבעזרתה תוכל להעריך את יעילותן של תוכניות האבטחה השונות, תוך השוואת העלויות של כל תוכנית ביחס לסיכוייה בהפחתת הסיכון לארגון. זה חשוב, מכיוון שבקרות מסוימות עלולות להיות יקרות מאוד, כדוגמת מערכת גז הלון לכיבוי שריפות, או בקרת כניסה אוטומטית - שלעתים אינן דרושות. בקרות אחרות דורשות בחירה בין גישות שונות לחלוטין, כמו במקרה של בחירה בין מערכות להצפת גז לבין מערכות להתזת מים.

אחת הבעיות הקשות ביותר באבטחה היא בקרה על תנועת האנשים, הזהה לבקרת כניסה. תחילה נדרשת החלטה של ההנהלה שתוביל לתוכנית אבטחה כוללת שאפשר להוציאה לפועל - אין זה מספיק לבקר את כניסת רוב האנשים. יש צורך לבקר את הכניסה של כולם. אם הפורץ הצליח להכנס לחדר המחשב מבלי להתגלות, לאחר שהושקעו סכומים צנועים באבטחה פיסית, אפשר להסיק שמשאבי החברה בוזבזו, מכיוון שבקרות הכניסה לא היו יעילות.

הנקודה השניה מתייחסת לעובדים: אלה חייבים להבין ולהסכים לבקרות הכניסה ולהיות מחויבים להצלחת התוכנית. הגבלת גישת העובדים עלולה ליצור דחייה מצידם ולגרום לירידה במוראל ולפגיעה ביעילות העבודה. תפעול יעיל של בקרות הכניסה מותנה, אם כך, בשיתוף הפעולה של העובדים.

במתקני מחשב רבים הותקנו בקרות כניסה פיסיות טובות, אך ההנהלה לא הצליחה להקצות את המשאבים הדרושים לניהול היומיומי, לאבטחה ולתחזוקה של אמצעי הבקרה. כדי למנוע מצב כזה, יש צורך בביקורת תקופתית של אמצעי האבטחה הפיסיים. יש לזכור: בנסיבות מסוימות, אמצעי האבטחה הפיסיים הם קו ההגנה העיקרי.

שאלות

2.1 במתקן מחשב ישנם גלאי חום לצורך גילוי אש. הסבר את היתרונות והחסרונות שבגישה זו.

2.2 בסעיף 1.4 נאמר שאמצעי הנגד מבצעים את הפונקציות הבאות: מניעה, גילוי, הרתעה, התאוששות, תיקון והמנעות. התייחס לאבטחה פיסית לפי פונקציות אלו.

2.3 סקר של שלושה מתקנים הראה שהראשון משתמש במבנה ישן שבו חלונות גדולים, הנמצאים בחזית, שמאחוריהם נמצא המחשב; השני נמצא במרתף, מתחת לקו המים של אפיק נחל סמוך; בשלישי יש חלונות גדולים, הוא נמצא במרתף ואפשר למצוא אצלו פגיעויות נוספות. מהן הפעולות שיש לנקוט בכל מקרה?

2.4 בצע "בדיקת קירבה" של מרכז המחשבים שלך ושל אתרים מרוחקים והגש דו"ח על ממצאיך (משימה קבוצתית).

2.5 בצע בדיקה במרכז המחשבים שלך, או בכל מתקן אחר, לגבי איזורים רגישים ובקרת הכניסה לאיזורים אלה והגש דו"ח על ממצאיך.



אין עשן בלי אש!

פרק 3

אבטחת נתונים

אבטחת נתונים עוסקת בשיטות להגנת נתונים במחשב ובמערכת התקשורת. בפרק 1 הראינו שאפשר להגן על מערכות מידע המבוססות מחשב רק אם מתקינים מנגנוני אבטחה מקיפים ויעילים בכל הסביבות הבאות:

(1) בתוך המחשב עצמו.
(2) במישק משתמש-מחשב.
(3) ברחבי הארגון שבו פועלת מערכת המידע.

בפרק זה ייסקרו מנגנוני אבטחה בתוך מערכת המחשב, כלומר הבקרות הפנימיות במחשב. בנוסף לכך, נדון בכמה בעיות הקשורות למישק משתמש-מחשב, מכיוון שהן משפיעות באופן ישיר על אבטחת הנתונים, בהחלשת בקרות פנימיות במחשב.

המחשב הוא מרכיב מרכזי במערכת המידע. יצרני ציוד וספקי תוכנה מספקים מאפייני חומרה ותוכנה שמאפשרים להגיע לרמת אבטחה מסוימת בתוך מערכת המחשב. בקרת סיסמאות ואימות משתמשים מסדירים את הכניסה למערכת המחשב במישק אדם-מחשב. אבטחת נתונים בתוך המחשב עצמו מתקיימת בעזרת ארבעה סוגים של בקרות (דנינג ודנינג, 1979; דנינג 1982):

* בקרת גישה
* בקרת זרימה
* בקרת ההיקש הלוגי
* בקרת הצפנה

בקרות גישה מפקחות על האובייקטים שמספקים הרשאת גישה למשתמשים מורשים. בקרות זרימה מנהלות את תנועת הנתונים מיחידת אחסון אחת לשניה. אסור שמשתמש יוכל לשלוף נתונים חסויים בעזרת היקשים לוגיים (inference) בבסיסי נתונים סטטיסטיים. שלורר (1979) הראה שבסיסי נתונים אלה פגיעים לסוג זה של התקפה הרבה יותר מבסיסי נתונים אחרים. לכן, חיוני להשתמש בבקרות היקש לוגי, למרות שהן רק מפחיתות את הסכנה ולא מבטלות אותה. יש להשתמש בהצפנה במקרים שבהם לנתונים אופי קריטי ובמקרים שבהם נדרשת הגנה נוספת על זו

שמסופקת על יד מנגנוני בקרה אחרים.

3.1 איומים לנתונים

האיומים לנתונים במערכות מחשב רבים, ביניהם (ראה גם טבלה 3.1):

* חיפוש ללא הבחנה.
* דליפה.
* היקש לוגי.
* הרס לא במכוון.

חיפוש ללא אבחנה וסריקה של אחסון משני נעשים בתקווה שימצאו תוכנה או נתונים שאמורים להיות חסויים ומוגנים. סוג זה של איום יכול להיות רק על ידי משתמש שיש לו גישה למחשב. לכן, בקרות גישה והצפנה יכולות לנטרל איום זה.

טבלה 3.1 איומים לנתונים המאוחסנים במחשבים ומנגנוני הגנה

סוג האיום	מנגנון הגנה
(1) חיפוש ללא הבחנה וסריקה	בקרת גישה
(2) דליפה	בקרת על זרימת הנתונים
(3) היקש לוגי (במיוחד בבסיסי נתונים סטטיסטיים)	בקרת ההיקש
(4) שינויים מכוונים	בקרת גישה והצפנה
(5) הרס לא במכוון	בקרת גישה
(6) התחזות	סיסמאות מוצפנות, חתימה דיגיטלית או שיטות ביומטריות אחרות.

שים לב! במקרים רבים, הקשורים לאיומים 2 ו-3, לא יספיקו מנגנוני האבטחה הרשומים מעלה ויש להשלימם בנוהלי התאוששות.

לתהליך עיבוד יכולה להיות הרשאת כניסה לאובייקטים מסוימים, והוא עלול לשחרר בטעות מידע או תוכנה למשתמש לא מורשה. דליפה עלולה להתרחש, לדוגמה, במהי'ך הידור של תוכנה מוגנת. בקרות על זרימת הנתונים, בנוסף לבקרת כניסה, יבטיחו שנתונים או תוכנה יחשפו רק לגורמים מורשים.

בסיס נתונים יכול לאחסן מידע רגיש וחסוי אודות אנשים או ארגונים. בסיס הנתונים אמור לספק סיכומים סטטיסטיים כתשובה לשאילתות של המשתמש, ובו זמנית - לשמור על סודיות הנתונים הקשורים לכל אדם ואדם. בסיס נתונים יכול לשחרר בטעות מידע סודי, אם הפורץ מציג סדרה של שאילתות בנויות היטב שניתן מתוך התשובות להן להקיש לגבי אדם מסוים. בקרות גישה וזרימה לא יכולות להתגונן בפני סוג זה של התקפה. קשה מאוד להגן על מידע חסוי, המאוחסן בבסיסי נתונים, בפני התקפה כזו, אבל בקרות היקש (שמתוארות על ידי פרננדז, 1981, ועל ידי צ'ין ואוזיוגלו, 1980) יכולות לעזור בהקטנת האיום. ניתן ליישם בקרות היקש, אבל אין בטחון ביעילותן, עם זאת, הן מקשות על עבודתו של הפורץ.

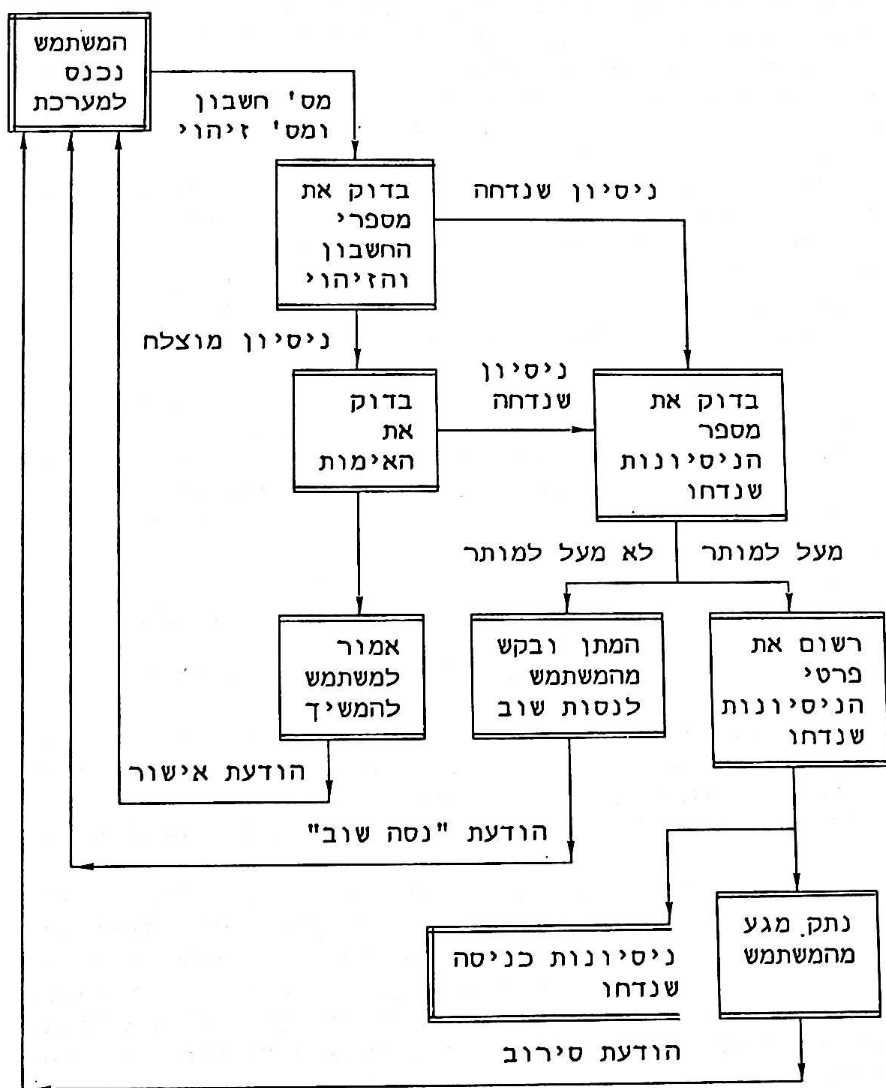
3.2 אבטחה במישק אדם-מחשב

3.2.1 זיהוי, אימות והרשאה של משתמשים

לפני שיופעלו מנגנוני הבקרה הפנימיים, על המשתמש לבקש הרשאה להכנס למחשב. נדרשת בקשה לזיהוי ולאימות של המשתמש או של האובייקט, לפני שמנגנוני הבקרה הפנימיים יוכלו להחליט על הענקת הרשאות גישה למשאבים מוגנים לאובייקט או למשתמש זה.

זיהויו של אובייקט, כמו מסוף, תוכנית או משתמש, נעשה בעזרת שם ייחודי שניתן לו, שלפיו המערכת מכירה אותו. הזיהוי הוא השלב הראשון בתהליך ההרשאה והוא נעשה בעיקר לצורכי התחשבנות. אולם זיהוי לבדו משתמשותי במידה מזערית מבחינת אבטחה, מכיוון שיש צורך לאמת את זהות המבקש. האימות מאשר שאדם או אובייקט הוא מי שהוא טוען שהוא. יש למלא אחר כמה דרישות לפני שזיהוי יתקבל כאותנטי (תהליך אימות טיפוסי מתואר בתרשים 3.1). מלבד מתקנים עם דרישות אבטחה גבוהות, האימות נעשה, כרגיל, רק פעם אחת במושב אחד (session). קיימות שלוש גישות בסיסיות לאימות משתמש:

(1) מאפיין ייחודי של המבקש, כמו קול או טביעת אצבעות.
(2) פריט הנמצא ברשות המבקש, כמו כרטיס מגנטי או מפתח.
(3) תהליך הידוע למבקש, כמו סיסמה.



תרשים 3.1 תרשים זרימה המראה את תהליך הזיהוי והאימות

הגישה הראשונה משתמשת בייחודיות של מאפיינים אישיים, לכן היא הבטוחה ביותר, אבל היא עדיין אינה נפוצה. הגישה השניה והשלישית נמצאות בשימוש נפוץ. תגים ומפתחות משמשים במצבים שבהם נדרשת רמה גבוהה של אבטחה, כמו למשל במחשוב בנקאי. בשילוב עם סיסמאות הם מספקים הגנה מצוינת.

3.2.2 סיסמאות

שיטה זו דורשת מהמשתמש להכניס מחרוזת של תווים שנבדקת על ידי המחשב. אם המילה שהוכנסה תואמת לסיסמתו של המשתמש שהכניס אותה, יספק לו המחשב הרשאה לכל האובייקטים שהוא מורשה להכנס אליהם.

סיסמה פשוטה דורשת מהמשתמש להכניס מחרוזת קצרה יחסית של תווים. פעולה זו קלה למשתמש ופשוטה לביצוע. המשתמש יכול לבחור את הסיסמה, אך יש לזכור שבמקרים כאלה משתמשים מתפתים לבחור במלה שקל להם לזכור, מצד אחד, ומצד שני - קל לפורץ לנחש אותה. לעתים, כאשר נבחרת סיסמה אקראית, הקשה יותר לזכירה, מתפתה המשתמש לרשום אותה על נייר, ובכך הופך אותה לפגיעה באותה מידה. ווד (1977, 1980) מסביר במאמריו בצורה מפורטת את החסרונות והיתרונות שבסיסמאות מסוגים שונים.

אם מגדילים את אורך הסיסמה, הופכים אותה ליותר בטוחה בפני פורץ המנסה לגלותה על ידי חיפוש שיטתי. הזמן הדרוש כדי לשבור סיסמה מוגדר על ידי הנדרסון (1972) והופמן (1977) כמקדם בטחון צפוי והוא:

(הזמן להכנסת סיסמה אחת) x (מספר הסיסמאות האפשריות) * 1/2

הנוסחה לחישוב הזמן שדרוש לשבור סיסמה בחיפוש שיטתי היא:

$$(1/2 \times N^{X}) * (L/T)$$

T = קצב הכנסת הנתונים ושידורם, תווים לדקה.
L = מספר התווים שיש להקליד בכל תהליך הכניסה (login).
X = אורך הסיסמה בתווים.
N = מספר האותיות והמספרים שמתוכם אפשר לבחור סיסמה.

בעזרת נוסחה זו ניתן לקבל אינדיקציה ליעילות האורך הנבחר של סיסמה, כפי שמתואר בדוגמאות הבאות.

דוגמה 3.1

חשב את מקדם הבטחון הצפוי אם פורץ מנסה לבצע חיפוש שיטתי באמצעות מקלדת.

הנח שקצב ההקלדה T שווה ל-120. מערכת התווים N היא בת 20 תווים (כלומר, נעשה שימוש רק במערכת מצומצמת של תווים). אורך הסיסמה X הוא 6 תווים. מספר התווים L, שיש להקליד

בתהליך הכניסה, הוא 15 תווים. בהתאם לנתונים, מקדם הבטחון הצפוי הוא:

$$(1/2 \times 20^6) \times (15/120) \text{ דקות}$$

$$= 4 \times 10^6 \text{ דקות} = 7.6 \text{ שנים}$$

דוגמה 3.2

חשב את מקדם הבטחון הצפוי כאשר ניסיון הפריצה מתבצע על ידי מחשב שני, המחובר למחשב הראשון שמשתמש בסיסמה. הנח שהנתונים זהים לאלה שבדוגמה 3.1, פרט לכך שקצב השידור T, בקו שבין שני המחשבים, הוא 1200 תווים לשניה. מקדם הבטחון הצפוי יהיה:

$$(1/2 \times 20^6) \times (15/72000) \text{ דקות}$$

$$= 6667 \text{ דקות} = 4.62 \text{ ימים}$$

בדוגמה השניה אנו רואים את השפעת המחשב על שבירת הסיסמה, ואת הצורך להשתמש בעיכוב (זמן המתנה) אוטומטי, לאחר כל ניסיון כושל. אפשר לראות זאת בתרשים 3.1. במקרה זה, ההמתנה בין ניסיון כושל לניסיון הבא היא קריטית. לדוגמה, אם זמן ההמתנה הוא 6 שניות, יתארך הזמן שנדרש להכנסת הנתונים בכל ניסיון מ-0.0125 שניות ל-6.0125 שניות. מקדם הבטחון הצפוי יגדל ליותר מ-6 שנים.

אפשר להרחיב את השימוש בגישה זו, כדי לחשב אורך סיסמה שיתאים לרמת הביצועים נדרשת. אם נניח שהסיכוי שתמצא סיסמה נכונה על ידי פורץ הוא p ופרק הזמן בחודשים שבו מתבצע החיפוש השיטתי כל יום במשך 24 שעות והוא M, יקבל p ערך נמוך יותר - p_0, השווה:

$$p_0 = \frac{\text{(מספר הניסיונות האפשרי לשבירת הסיסמה ב-M חודשים)}}{\text{(מספר הסיסמאות האפשריות)}}$$

מספר הניסיונות האפשרי ב-M חודשים $= [T(M \times 30 \times 24 \times 60)] / L$

מספר הסיסמאות האפשריות $= N^x$

ולכן:

$$p = (4.32 \times 10^4 \times T \times M) / (L \times N^x)$$

הסיכוי שתמצא סיסמה נכונה הוא p, כאשר $p \geq p_0$. מכאן אנו מגיעים לנוסחת אנדרסון:

$$N^x \geq (4.32 \times 10^4 \times T \times M) / (L \times p_0)$$

אפשר להשתמש בנוסחה זו כדי לבחור את אורך הסיסמה, X, כך שהסיכוי שפורץ יגלה סיסמה לא יהיה גדול יותר מ-p, כפי שמתואר בדוגמה הבאה.

דוגמה 3.3

חשב את אורך הסיסמה אם גודלה של מערכת התווים הוא 26 תווים, והסיכוי שהסיסמה תתגלה, לאחר חודש אחד של התקפה שיטתית, לא יעלה על 0.001. קצב הכנסת הנתונים הוא 300 תווים בשניה, ויש להקיש 15 תווים בתהליך הכניסה.

אם נשתמש במשוואה שבדוגמא הקודמת, נקבל:

$$26^x \geq (4.32 \times 10^4 \times 300 \times 1) / (15 \times 0.001) =$$

$$26^x \geq 8.64 \times 10^8$$

אם x שווה ל-6 נקבל:

$$26^x = 3.09 \times 10^8$$

אם x שווה ל-7 נקבל:

$$26^x = 8.03 \times 10^9$$

תוצאות אלו מצביעות על הצורך להשתמש בסיסמה שאורכה 7 תווים לפחות.

משלוש הדוגמאות שהובאו, אפשר ללמוד את הדברים הבאים:

(1) הגורם המכריע במניעה מפורץ מלגלות סיסמה על ידי חיפוש שיטתי, הוא אורך הסיסמה.
(2) סיסמאות, גם אם הן בנות חמישה עד שישה תווים, בטוחות יחסית בפני התקפה שיטתית.
(3) סיסמה לא תחשף, בדרך כלל, על ידי התקפה שיטתית, אלא כתוצאה מחוסר זהירות של משתמשים.

3.2.3 סיסמאות בטוחות יותר

קיימות גירסאות רבות לסיסמה המסורתית, שמספקות הגנה טובה יותר, אך מקשות על המשתמש. הן כוללות הכנסת תווים נבחרים מתוך הסיסמה וסיסמאות חד פעמיות. ווד (1980) דן במאמריו בגירסאות אלו ובאחרות. בטבלה 3.2 תמצא סיכום של מאפייניהן.

בשיטה הראשונה מתבקש המשתמש להכניס רק מספר תווים נבחרים מתוך הסיסמה. תווים אלה משתנים בכל ניסיון כניסה. לכן, סכוייו של פורץ, שמשיג מידע לגבי ניסיון כניסה אחד, להכנס למערכת מעטים מאוד, כי יש לו מידע מניסיון כניסה אחד, שכתוצאה ממנו הוא מחזיק רק בחלק מהסיסמה.

הסיסמה החד פעמית מורכבת יותר, ובהתאמה - גם בטוחה יותר. המשתמש מקבל רשימה של סיסמאות והוא יכול להשתמש בכל סיסמה מהרשימה רק פעם אחת, לפי סדר שנקבע מראש. אם המשתמש קיבל את הסיסמאות X12, X74, X01 ו-X11, המערכת מצפה שלאחר שהוא השתמש ב-X12 הוא ישתמש ב-X74. כל סיסמה אחרת תדחה. החסרון העיקרי של שיטה זו הוא שהמשתמש חייב לזכור, או לרשום על נייר, את כל רשימת הסיסמאות וכן, לעקוב אחר סדר הכנסת הסיסמאות. ללא קשר לסוגי הסיסמאות שנבחרו, חובה להגן עליהן בעזרת הכללים הבאים, שמתוארים בפרוטרוט במאמריהם של ווד (1980) והופמן (1977):

(1) יש להצפין סיסמאות שנשמרות במערכת המחשב.
(2) אין להציג סיסמה במסך, או להדפיס אותה על גבי תדפיסי מחשב. אם אין ברירה אחרת, יש להדפיס עליה שוב, כדי שפורץ לא יוכל להבין את הכתוב.
(3) כפי שכבר צויין, ככל שאורך חיי הסיסמה גדול יותר, כך גדל הסיכוי לגלות אותה. לכן, יש לשנות אותן בתדירות גבוהה, בהתחשבות בנסיבות מקומיות.
(4) יש להנפיק את הסיסמאות דרך ערוץ תקשורת מאובטח. לדוגמה, אין להנפיק סיסמה בסוף מושב (session) של משתמש, כי ייתכן שהמסוף מופעל על ידי פורץ.

אפשר להשתמש בסיסמה לא רק כדי לאמת משתמש למערכת ההפעלה, אלא גם כדי לאמת מחשב למשתמש. כדי להבטיח שהמשתמש התקשר למחשב הרצוי ולא למחשב של פורץ לרשת, על המחשב להחזיר למשתמש סיסמה. יש להחליט מראש על הסיסמה עם המשתמש.

טבלה 3.2 מאפיינים של שיטות אימות

מאפיין האימות	יתרונות	חסרונות
תהליך בחירת הסיסמאות		
(1) על ידי המשתמש (2) על ידי המערכת	קל לזכור קשה לנחש	קל לנחש קשה לזכור
אורך חיי הסיסמה		
(1) לא מוגדר	קל לזכור	פגיעה לחיפוש שיטתי ואם נחשפה, לא ברור אם זה כתוצאה מחיפוש או מחוסר תשומת לב.
(2) פרק זמן קבוע	קל לזכור אותה והיא יותר בטוחה מסיסמה שאורך חייה אינו מוגדר	הפגיעות תלויה באורך פרק הזמן שנקבע
3) סיסמה חד פעמית	אין אפשרות לשבור אותה בעזרת חיפוש שיטתי	קשה לזכור אותה; אם הסיסמה נחשפה, ייתכן שמשתמש מורשה ינותק מן המערכת.
אורך הסיסמה וגודל מערכת התווים		
סיסמה ארוכה יותר ומערכת תווים גדולה יותר	קשה יותר לנחש, או לשבור אותה	קשה לזכור אותה, לכן קיים סיכוי סביר שהמשתמש ירשום אותה.
Handshaking (לחיצת יד) דיאלוגים וטרנספורמציות	עמיד יותר בפני חיפוש שיטתי	השקעה גדולה יותר של זמן ושל כסף.

3.2.4 לחיצת יד (Handshaking)

שיטת אימות שמספקת אבטחה ברמה גבוהה יותר מסיסמאות, היא תהליך לחיצת יד. ניתן לבצעו בין שני מחשבים, או בין משתמש למחשב. בלחיצת ידיים מקבל המשתמש נוסחת היפוך (transform) t_u שידועה למחשב. לדוגמה, כאשר המשתמש רוצה להכנס למערכת, המחשב מגיב במשלוח המספר y (שנבחר בצורה אקראית) למשתמש, ומבקש תשובה. התשובה הדרושה תהיה $t_u(y)$. אם פורץ משיג את הערכים של y ושל $t_u(y)$, הוא יתקשה עדיין למצוא את הנוסחה t_u. הופמן הציג שיטת היפוך פשוטה:

$$T(y) = \left[\left(\sum_{\text{אי-זוגי } i} (\text{ספרה } i \text{ של } y) \right)^{1.5} \right] + (\text{שעה ביום})$$

לדעתו, היא מגדילה באופן משמעותי את המאמץ הדרוש לשבירת תהליך האימות. תהליך לחיצת הידיים צורך זמן ממושך יותר, והוא בטוח כל עוד נשמרת הסודיות של נוסחת ההיפוך.

3.3 בקרת כניסה לנתונים

3.3.1 הצורך בבקרת כניסה

לאחר שמשתמש עבר בהצלחה את תהליך האימות, הוא ינסה להכנס לאובייקטים השונים. קיימים אובייקטים ששייכים למשתמש, כמו קובץ, רשומה או תוכנית, וקיימים אובייקטים ששייכים למערכת, כמו קבצים, סגמנטים של זיכרון, או סביבה מוגנת שמתבצע בה תהליך מסוים. יעילות הבקרות תלויה בהגנה על האובייקטים של המשתמש ועל המערכת. לכן חיוני שכל בקשת כניסה תבדק, כדי להבטיח שאפשר לאשר אותה. אישור תלוי בגורמים הבאים:

* אם המשתמש קיבל הרשאת כניסה מסוימת.
* הרשאות הכניסה של המסוף שדרכו נכנס המשתמש למערכת.
* הפעולה שהמשתמש ביקש לבצע, כמו קריאה או כתיבה.
* הנתון וערכו.
* היום, או שעה ביום.

לבקרת הכניסה שני היבטים שקשורים ביניהם:

(1) המדיניות שמכתיבה את הרשאות הכניסה.
(2) המנגנונים שבעזרתם נאכפת המדיניות הזו.

3.3.2 טבלת הרשאות ומדיניות בקרת כניסה

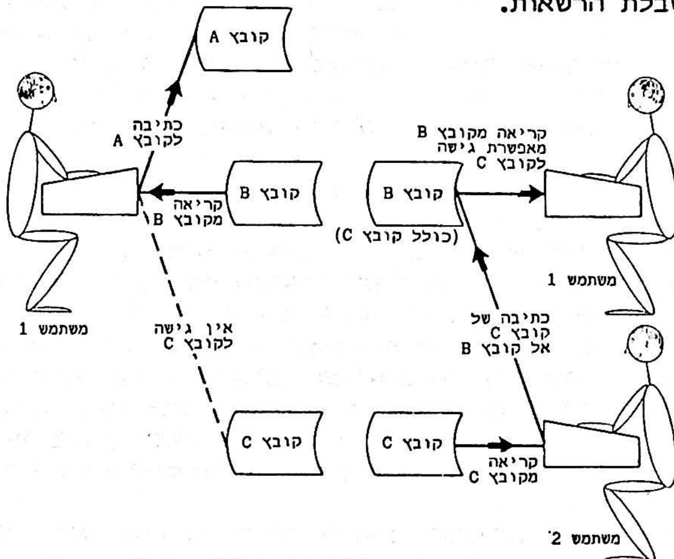
מודל טבלת ההרשאות הוא תוכנית מסגרת לציון מערכות ההגנה במערכת ההפעלה (למפסון, 1971) ובבסיס נתונים (קונווי, 1972). המודל מוגדר במונחים הבאים:

(1) מצב מערכת ההגנה.
(2) שינויי מצב.

מצב מערכת ההגנה (דנינג ודנינג, 1979) מיוצג בעזרת שלוש אותיות - A, O, S - שמשמעותן:

S נתינים (subjects), שהם יישויות פעילות במודל.
O אובייקטים (objects), שהם יישויות פסיביות המוגנות במערכת ומזוהות בעזרת שם ייחודי.
A טבלת ההרשאות, שייצוג בה בצורה של A[s,o] מבטא את הרשאת הכניסה לנתין s אל אובייקט o.

במערכת ההפעלה, אובייקטים הינם יישויות שיש צורך לבקר את הכניסה אליהם. הם כוללים: קבצים, אמצעי אחסון חיצוניים, סגמנטים של זיכרון, תוכניות והפעלה של תוכניות. הנתינים, שכוללים משתמשים, תהליכים ותוכניות, הם יישויות שמבקשות להכנס לאובייקטים (ראה גם תרשים 3.2). דוגמאות להרשאות כניסה יכולות להיות קריאה, כתיבה וביצוע. תרשים 3.3 מתאר חלק מטבלת הרשאות.



תרשים 3.2 גישה למידע וזרימת מידע

נתינים	קובץ 1	סגמנט זיכרון 1	סגמנט זיכרון 2	התקן 1	נתין 1	נתין 2
	אובייקטים					
נתין 1	בעלים קריאה כתיבה	ביצוע קריאה כתיבה		מחפש		קורא
נתין 2		קריאה	ביצוע קריאה כתיבה			

תרשים 3.3 טבלת הרשאות

אחת הגישות לאבטחת בסיס נתונים היא לראותה כהרחבה של אבטחת מערכת ההפעלה. יש להגדיל, לפיכך, את כמות האובייקטים בטבלת ההרשאות ולכלול בהם פריטים ששייכים לבסיס הנתונים. הבדלים רבים קיימים בין אבטחה של מערכת ההפעלה לבין אבטחה של בסיס נתונים. נמנה כמה מהם:

* בבסיס הנתונים יש להגן על מספר גדול יותר של אובייקטים.
* האובייקטים יכולים להיות מבנים לוגיים מורכבים (מול משאבים אמיתיים במערכת ההפעלה).
* אורך החיים של הנתונים בבסיס הנתונים ארוך יותר, בדרך כלל.
* אבטחה של בסיס נתונים מטפלת בכמה רמות של כניסה, כמו שדה, רשומה או קובץ.

אבטחת בסיס הנתונים נמצאת באחריות המערכת לניהול בסיס נתונים. בסיס הנתונים משתמש במאפייני האבטחה הבסיסיים, שמסופקים על ידי מערכת ההפעלה ויש ליצור טבלת הרשאות מיוחדת לבסיס הנתונים (ראה תרשים 3.4). טבלת ההרשאות של בסיס הנתונים סטטית יותר מזו של מערכת ההפעלה. הנתינים הם משתמשי קצה, קבוצות של משתמשים, או תוכניות המבצעות בקשות של המשתמשים. בין ההרשאות האופייניות: קריאה, כתיבה, עדכון, הוספה או ביטול. הערך A[s,o] מצביע על הפעולות שהמשתמש יכול לבצע על האובייקט o והאם הוא מורשה לגשת לאובייקט o.

ההרשאות לא קשורות תמיד למהות הנתונים, בדומה למערכת ההפעלה, והן יכולות להיות תלויות בהם. פירוש הדבר הוא שיש להתחשב בערכי הנתונים (הרטסון והאיסו, 1975). לדוגמה, משתמש

מורשה לקרוא את שדה המשכורת בכל אחת מרשומות העובדים שמשכורתם היא 15,000 שקל או פחות, אבל אין הוא מורשה לקרוא את המשכורת אם היא גדולה מ-5,000 שקל. בקרה שתלויה בנתונים גורמת שתתבצע בדיקת אבטחה בכל פעם שיש דרישה לנתון בזמן העיבוד. עובדה זו מגדילה באופן משמעותי את זמן העיבוד, בהשוואה לבקרת כניסה שאינה תלויה במהות הנתונים. אפשר לצמצם את הזמן העודף בעזרת שגרות קלט/פלט ובאופי הנתונים (וודוורד והופמן, 1974).

הגבלות אחרות יכולות להיות מותנות בזמן העבודה ובגיל המשתמש. דוגמאות לכך יכולות להיות הרשאות גישה לרשומות של משכורות רק בין השעות 9 בבוקר ל-5 אחה"צ, או הרשאות כתיבה בקובץ בלתי מסווג, בתנאי שהוא לא קרא קודם לכן מתוך קובץ המכיל נתונים מסווגים.

אחד הדברים שחיוני להקפיד עליהם הוא בקרה של הנוהלים שמשנים את טבלת ההרשאות. לצורך זה הוצע מודל המבוסס על שש פקודות: הכנסת הרשאה, ביטול הרשאה, יצירת נתין או אובייקט וביטול נתין או אובייקט (הריסון, 1979).

יש לזכור שאין חובה לאחסן את טבלת ההרשאות בצורת טבלה מכיון שאחסון כזה הוא בזבזני מבחינת מקום. מודל טבלת ההרשאות הוא ייצוג מופשט של מדיניות האבטחה.

	פרטי העובד					
נתינים	שם	כתובת	מספר	כישורים	מספר טלפון	משכורת
כוח אדם	קריאה כתיבה	קריאה כתיבה	קריאה כתיבה	קריאה כתיבה	קריאה כתיבה	קריאה
מנהל חשבונות	קריאה	קריאה	קריאה		קריאה	קריאה כתיבה
מתכנן			קריאה			

תרשים 3.4 טבלת הרשאות לבסיס נתונים

3.3.3 מנגנוני בקרת כניסה

עקרונות התכנון של מנגנוני ההגנה נקבעו על ידי סלצר ושרודר (1975). הם כוללים:

(1) מספר הרשאות קטן ככל האפשר. יש להקצות לכל נתין רק את ההרשאות הדרושות לו להשלמת העבודה. בכך מוגבל הנזק שיכול להגרם משגיאה או מהתקפה ונדרש שתהליכים יתבצעו בתחומים (domain) קטנים ומוגנים. ברירת המחדל צריכה להיות "אין הרשאה", כלומר אין רשות לגשת. בנוסף לכך, עיקרון זה עוזר להתמודד עם "סוסים טרויאניים" - תוכניות שמכילות פקודות לא רצויות שאינן מתוארות במפרט שלהן (לינדן, 1975).

(2) חישוב כלכלי. טוב יותר להתקין מנגנון פשוט יחסית, ממנגנון בעל מאפיינים מורכבים ומתוחכמים, שמשתמשים בהם לעתים רחוקות בלבד.

(3) תכנון לא סודי. רמת האבטחה אינה צריכה להיות תלויה בסודיות של התכנון (ברן, 1964). אם אי אפשר לתאר את המערכת בעיתונות מבלי לפגוע באבטחה, השימוש בה אינו בטוח (מאפיין זה הוא במפורש אחד ממאפייני UNIX, מיום שיצאה לראשונה לאור).

(4) כל בקשה לכניסה חייבת להבדק ולקבל אישור, בהתאם לרמת ההרשאות של המבקש. המנגנון חייב להיות יעיל, כדי שמשתמשים לא יוכלו למצוא דרך שתעקוף אותו.

(5) הפרדה של הרשאות. כניסה לאובייקטים צריכה להיות תלויה ביותר מתנאי אחד, היכן שאפשר.

(6) פשוט לתפעול. מנגנונים צריכים להיות פשוטים לתפעול, מתוכננים באופן שבו הגבלת הכניסה לאובייקטים לא תהיה מסובכת יותר מאשר להשאיר אותם פתוחים.

מספר מזהה של המשתמש	הרשאות
UG07	קריאה, כתיבה
UG09	קריאה
US01	קריאה
US02	בעלות,קריאה,כתיבה
US03	קריאה

תרשים 3.5 רשימת הרשאות לקובץ

קיימים שלושה סוגים של מנגנוני בקרה (דנינג, 1982) שמבוססים על התפישות הבאות:

(1) הירכיה של הרשאות.
(2) רשימת הרשאות.
(3) אפשרויות ביצוע.

בהירכיה של הרשאות, ניתנים לנתינים עם סיווג גבוה הרשאות רבות יותר מאלה שניתנות לנתינים עם סיווג נמוך יותר. מצב מועדף (supervisor state) הוא מנגנון בקרת כניסה שמבוסס על גישה זו. ברוב המערכות קיים מצב מועדף, שמאפשר לתוכניות הרצות עם סיווג כזה להכנס לכל אובייקט במערכת. מצב מועדף אינו עומד בעיקרון של מספר ההרשאות קטן ככל האפשר, מכיוון שלתוכניות של מערכת ההפעלה יש הרשאות רבות יותר מהדרוש להן לביצוע משימותיהן. בכל זאת, מצב מועדף שיפר את האבטחה במערכות רבות, במחיר נמוך. אבל, אם נדרשת רמת אבטחה גבוהה, יש צורך במנגנונים נוספים שיגבילו את הרשאות הכניסה של תוכניות הפועלות במצב מועדף.

רשימת הרשאות, או רשימת בקרת כניסה, היא רשימה של נתינים שמצורפת אליה הרשאה של כל אחד מהם להכנס לאובייקט מסוים. לכן, רשימת הרשאות מייצגת ערכים בטבלת הרשאות, שמשתמשים בהן, בדרך כלל, להגנה על אובייקטים שיש להם בעלים, כמו קבצים. רשימת הרשאות לקובץ כוללת את שמות המשתמשים, או הקבוצות המורשות, ואת ההרשאות שיש לכל משתמש (ראה גם תרשים 3.5). במערכות רבות קיימת צורה מנוונת של רשימת הרשאות שבה יש רק שני ערכים: האחד מציין זכויות בעלות והשני מציין את הרשאות הכניסה לכל שאר המשתמשים. מנגנון כזה אינו עומד בעיקרון של מספר הרשאות קטן ככל האפשר, אבל רשימת הרשאות מנוונת קלה יחסית ליישום ומספקת במצבים רבים. חיפוש ברשימת הרשאות עלול להמשך זמן רב ולכן, מערכות רבות אינן בודקות את הרשימה בכל כניסה. רשימות הרשאה אינן מתאימות להגנה על סגמנטים של הזיכרון.

גישת אפשרויות הביצוע מבוססת על מתן הרשאות לנתינים. הבעלות על הרשאה מזכה באופן אוטומטי את המחזיק בה ברשאת גישה לאובייקט מסוים. אפשרות הביצוע מיוצגת על ידי זוג ערכים (o,p) המציינים שהמחזיק בה מורשה, ללא תנאי, להיות בעליהן של הרשאות כניסה p לאובייקטים o. אפשר ליישם את גישת אפשרויות הביצוע ברמת הפרוצדורה מכיוון שהיא ממלאה את עיקרון התכנון של מספר ההרשאות קטן ככל האפשר.

3.3.4 בעיות ביישום של מנגנוני בקרת כניסה

הסיווג הגבוה ביותר, מבחינת הרשאות, שניתן למערכת ההפעלה, הוא בעיה נפוצה וחמורה. מצב מועדף עוקף את כל מנגנוני ההגנה של אמצעי האחסון והוא עומד בסתירה לעיקרון של מספר הרשאות קטן ככל האפשר.

בעיה נוספת היא כפייה על משתמשים להכניס אובייקטים לתוך סגמנטים גדולים בזיכרון, שאינה מאפשרת להגן על סגמנטים קטנים ומסוימים בזיכרון. החומרה אינה מתוכננת לספק בקרת כניסה יעילה, מכיוון שניהול של סגמנטים קטנים בזיכרון גורם עומס יתר במערכת ומקשה על יישום העיקרון של רשימת אפשרויות לכל תוכנית.

קיימים קשיים נוספים בנושא בקרת כניסה, ביניהם: בדיקה שהיישום עונה על הדרישות של מדיניות בקרת הכניסה (גיינס ושפירו, 1978), והצורך לדאוג שהצרכים של המשתמשים יהיו תמיד ביחס ישר להרשאות הניתנות להם (סניידר, 1981).

3.4 בקרת זרימה (Control of flow)

3.4.1 בקרות זרימה כתמיכה במנגנוני בקרה אחרים

זרימה של נתונים מאובייקט A לאובייקט B מתרחשת כאשר נקראים נתונים מאובייקט A ונכתבים לאובייקט B, כתוצאה מרצף של הוראות. העתקה של קובץ A לקובץ B, כפי שאפשר לראות בתרשים 3.2, היא תיאור פשוט של זרימת מידע. אפשר לאכוף נוהלי בקרת כניסה קפדניים מאוד, אך ברור מהדוגמה שבקרת כניסה לבדה אינה מספקת כדי לשלוט בפעולות שנתינים יכולים לבצע עם המידע הנמצא באובייקטים שאליהם נכנסו. מידע עלול לדלוף אפילו כאשר קיימים במערכת מספיק מנגנוני בקרת כניסה, מכיוון שעלול להיות פגם בבקרות של זרימת הנתונים. מדיניות בקרת זרימה מציינת את הערוצים, ביחד עם המידע המורשה לעבור בהם.

3.4.2 מדיניות זרימת המידע

קווי מדיניות זרימה טיפוסיים מציינים את הפרטים הבאים:

(1) שתי רמות מידע: אובייקטים סודיים ולא סודיים.
(2) כמה רמות סודיות המשולבות עם קטגוריות של נתונים.

במדיניות הכוללת שתי רמות מידע, זרימת המידע מותרת בכל

המקרים, מלבד אלה שבהם כיוון הזרימה הוא מאובייקטים סודיים לאובייקטים לא סודיים.

השיטה השניה, מדיניות אבטחה עם מספר רמות הרשאה, נחוצה לעתים קרובות במערכות המאחסנות מידע צבאי או ממשלתי. כל רמת אבטחה מיוצגת על ידי זוג ערכים (L ,C) כאשר L מציין את רמת הסודיות ו-C מציין את הסיווג של הנתונים. שיטה זו מאפשרת להגן על המידע באופן הירככי ובעזרת סיווגים ייחודיים (הרטסון והסיו, 1975). רמות הסודיות יכולות להיות סודי ביותר, סודי, שמור ולא סודי, וסיווגי הנתונים יכולים להיות C1, C2, C11...C12. זרימת נתונים תתבצע מאובייקט בעל רמת אבטחה Lx,Cx לאובייקט בעל רמת אבטחה Ly,Cy בתנאי ש-Ly≥Lx ובתנאי שסיווגי הנתונים Cx קיימים גם ב-Cy. דבר זה מתואר בתרשים 3.6.

3.4.3 מנגנונים המשמשים לבקרת הזרימה של נתונים

אפשר לקבוע מנגנונים שיאכפו את מדיניות האבטחה בנקודות הבאות:

(1) בזמן הביצוע, על ידי אימות כל מסלולי הזרימה במהלך התרחשותם (ויצמן, 1969).

(2) בזמן ההידור, על ידי בדיקת כל מסלולי הזרימה לפני התרחשותם; כלומר, לפני שהתוכנית מתבצעת (דנינג ודנינג, 1977).

אובייקט	רמת סודיות	סיווג של נתונים
ל-X יש רמת אבטחה...	שמור...	C14, C11, C6, C5, C2
ל-Y יש רמת אבטחה...	סודי...	C10, C1, C2
במקרה זה זרימת הנתונים היחידה המותרת מ-X ל-Y	סודי...	C2
זרימת הנתונים מ-Y ל-X אינה מותרת		

תרשים 3.6 בקרת זרימה המבוססת על מספר רמות של אבטחה

אפשר להתקין את השיטה הראשונה ביחד עם בקרות הכניסה של מערכת ההפעלה. היא דורשת שלכל תוכנית תנתן רמת הרשאה שתציין את הרמה הגבוהה ביותר של זיכרון, שמתוכה היא יכולה לקרוא. בדומה, אישור כתיבה לסגמנט יינתן רק אם רמת ההרשאה של הסגמנט המקבל זהה לזו של התוכנית. שילוב התנאים מבטיח שהתוכנית לא תוכל לשדר מרמת אבטחה גבוהה לרמת אבטחה נמוכה. לצערנו, היא מאפשרת לנתונים לנוע כלפי מעלה. אפשר לצמצם בעיה זו אם מאפשרים לתוכנית שרצה להתחיל ללא הרשאה ולטפס (אך לעולם לא לרדת), עד לרמת האבטחה הגבוהה שנקבעה לה. אין זה מבטל לגמרי את הבעיה של סיווג יתר, מכיוון שלאחר שהתוכנית הגיעה לרמה מסוימת היא לא תוכל לרדת ממנה.

כדי לאכוף מדיניות נוקשה לבקרת זרימה, יש צורך להשתמש במנגנונים בעלי אפשרויות סיווג מפורטות יותר של תוכנה וחומרה (פנטון, 1974). למרות זאת, מנגנונים לבקרת כניסה מורחבת פועלים מסוף שנות ה-60 (וויצמן, 1969).

3.4.4 קשיים עם בקרות זרימה

נקודות התורפה של מנגנונים המשמשים לבקרת הזרימה של המידע כוללות:

(1) סיווג בבניית מידע.
(2) הקושי בתהליך אוטומטי להורדת רמת האבטחה, כבסיס לשחרור מידע בעל רמה נמוכה.
(3) מידע הזורם בערוצים חסויים - covert channels - (למפסון, 1981).

מנגנונים לבקרת כניסה מורחבת אינם מאפשרים למידע לזרום כלפי מטה. כתוצאה מכך, הדרך היחידה שבה אפשר להוריד את רמת הסודיות של נתונים היא ידנית בהתערבות של משתמש מורשה שיעקוף את מנגנוני ההגנה. אפשר להשתמש גם בתוכניות מיוחדות שיורידות את רמת הסודיות של המידע. מתוך הסעיף הבא, שעוסק בבקרות ההיקש אפשר להבין, שתוכניות רבות שתפקידן הוא לסנן נתונים לרמות נמוכות יותר של סודיות, אינן עושות זאת.

תוכנית יכולה להעביר מידע לצופה באמצעות שינויו והפיכתו לתופעה פיסית, כמו שינוי של נתונים סודיים, לשם הצגתם המהלך הריצה של תוכנית. סוג זה של זרימה משתמש בערוצים חסויים וקשה מאוד לשלוט בו. פתרון אחד דורש שכל עבודה (job) רצה תתן הערכה של המשאבים הדרושים לה ושל זמן העיבוד המשוער, כדי שתוכל להמשיך ולהתבצע.

3.5 בקרות היקש לוגי

3.5.1 הגדרה

מערכת מידע רפואי יכולה להשתמש בבסיס נתונים סטטיסטי לצורך קבלה של מידע סטטיסטי רפואי, מבלי לחשוף מידע הקשור לחולה מסוים. לצערנו, ניתן למצוא בדוחות הסיכום עקבות של מידע מקורי. פורץ יוכל לשחזר מידע לגבי חולה בעזרת עיבוד והשוואה של מספר סיכומים. עובדה זו מהווה איום לפרטיותו של אדם, כי בעזרת היקש לוגי אפשר להגיע למידע חסוי. אי אפשר לבטל את כל האיומים של היקש לוגי, ולכן המטרה של בקרות אלו היא להקשות על פורצים ולגרום להם נזק כספי ניכר, אם הם ינסו לשלוף מידע חסוי.

3.5.2 דוגמה של חשיפת נתונים מתוך בסיס נתונים

שים לב ל"שיחה" בין משתמש לבין בסיס נתונים רפואי:

שאלה: כמה אנשים בבסיס הנתונים מחזיקים במאפיינים הבאים:
- זכר
- רווק
- גיל: 40 - 35
- גובה: 6 רגל
- משקל: 76 ק"ג
- מקצוע: עורך דין

תשובה: 1

בהנחה שהעבריין - המשתמש מכיר את העובדות הללו על מר סמית, הוא יוכל להמשיך בדיאלוג, כדי לנסות לגלות מידע חסוי אודותיו. לדוגמה, אם מגדילים את רשימת המאפיינים בשאלה המקורית, כדי שתכלול גם מחלה רצינית אחת, התשובה של 1 מבסיס הנתונים תצביע על כך שמר סמית סבל מהמחלה, ו-0 יצביע על כך שאינו חולה. הדוגמה מראה כיצד עבריין בעל תושייה יכול להשיג מידע חסוי מבסיס נתונים. חוקרים רבים הוכיחו שבסיסי הנתונים פגיעים הרבה יותר ממה שניתן לשער.

3.5.3 איומים לבסיסי נתונים

בסיס נתונים מכיל רשומות שחלק מהמאפיינים שלהן חסויים ודורשים הגנה. כאשר מתבצעת שאילתה סטטיסטית, בסיס הנתונים אינו עונה עם מאפיינים מפורטים, אלא רק עם סיכומים

סטטיסטיים לגבי מאפיינים אלה. כל שאילתה היא ביטוי לוגי המשתמש באופרטורים לוגיים. התשובה היא קבוצה של רשומות שעומדת בדרישות הביטוי ושמה "קבוצת השאילתה" (query set).

חוקרים הראו שקיימות דרכים רבות לשליפת מידע חסוי מבסיס נתונים. בין שיטות ההתקפה שזוהו:

(1) קבוצת שאילתה קטנה.
(2) קבוצת שאילתה גדולה.
(3) הכנסת רשומות מדומות.
(4) עוקב (tracker).
(5) משוואות סימולטניות שמנתחות את התשובות.

הדוגמה של פגיעה בבסיס הנתונים, שהובאה בסעיף 3.5.2, אפשרית מכיוון שתשובת בסיס הנתונים היא קבוצת שאילתה קטנה המאפשרת לבודד אדם מסוים (הופמן ומילר, 1970). בהנחה

שמספר האנשים המחזיקים בתכונה P_q בשאילתה הוא $N(P_q)$

שמספר האנשים $N(C)$ המחזיקים בתכונות $P_1, P_2,...P_n$

כלומר אם המאפיין נתון על ידי: $C = (P_1 \wedge P_2 \wedge P_3 \wedge \ ... \wedge P_n)$

$$N(C) = N(P_1 \wedge P_2 \wedge P_3 \wedge ... \wedge P_n)$$

ואז ניתן לבודד אדם מסוים, אם ידוע ששהוא מחזיק בתכונות:

$$P_1, P_2, ...P_k$$

וגם המאפיין:

$$N(P_1 \wedge P_2 \wedge ... \wedge P_k) = 1$$

חטטן יבקש את מספר האנשים בבסיס הנתונים המחזיקים בתכונה P_x, שתתווסף לשאילתה הקודמת. אם התשובה תהיה:

$$N(P_1 \wedge P_2 \wedge ... \wedge P_k \wedge P_x) = 1$$

משמעות הדבר היא שהאדם המסוים, שאליו מתייחס המידע החסוי, מחזיק בתכונה P_x.

סוג אחר של התקפה, שאפשרי אם מותרת קבוצת שאילתה קטנה, הוא הצבה של אדם מסוים בקבוצה קטנה המחזיקה בתכונה מסוימת. במקרה כזה אין צורך לקבוע את התכונות הייחודיות לזיהויו של

אדם מסוים זה, די אם נקבע שהוא מחזיק ב-i תכונות. העבריין יקבל את התשובה הבאה, לגבי i תכונות

$$N(P_1 \wedge P_2 \wedge \ldots \wedge P_i) > 1$$

לאחר מכן מתבצעות שאילתות נוספות המחזיקות בתכונה Px, בנוסף ל-i תכונות. אם

$$N(P_1 \wedge P_2 \wedge \ldots \wedge P_i \wedge P_x) = N(P_1 \wedge P_2 \wedge \ldots \wedge P_i)$$

משמעות הדבר היא שאדם מסוים מחזיק בתכונה P_x.

הדוגמאות שהובאו מראות שיש להחזיר תשובה לשאילתה, רק אם קבוצת השאילתה גדולה מהמספר השלם Nmin. אולם אין די בהגבלת הגודל בתשובות המותרות ליותר מאשר Nmin, מכיוון שקבוצת שאילתה גדולה, הקרובה לגודל בסיס הנתונים עלולה גם היא לפגוע בבסיס הנתונים. תאר לעצמך מצב שבו אנשים רבים בקובץ המחזיקים בתכונה Px. עבריין רוצה לגלות אם פרט מסוים מחזיק בתכונה Px, קבוצת שאילתה קטנה אינה מותרת, וידוע שאפשר לזהות פרט מסוים בעזרת המאפיינים C שמקיימים:

$$C = (P_1 \wedge P_2 \wedge P_3 \wedge \ldots \wedge P_n)$$

העבריין שואל על מספרם הכולל של האנשים המחזיקים בתכונה P_x, כלומר:

$$NT = N(P_x)$$

אם נשאלת שאלה דומה שהתשובה עליה N_{T-I}, האדם יהיה בעל התכונה Px, אם מתקיים השוויון:

$$(NT - N_{T-I}) = 1$$

אפשר למצוא את הערך של N_{T-I} על ידי שאלה על מספר האנשים שמחזיקים בתכונות הבאות:

$$(\bar{P}_1 \vee \bar{P}_2 \vee \bar{P}_3 \vee \ldots \vee \bar{P}_n) \wedge P_x$$

התשובה תהיה N_{T-1}. זה נכון כי לפי חוקי דה-מורגן מתקיים השוויון:

$$(\bar{P}_1 \vee \bar{P}_2 \vee \bar{P}_3 \vee \ldots \vee \bar{P}_n) \wedge P_x = \overline{(P_1 \wedge P_2 \wedge P_3 \wedge \ldots \wedge P_n)} \wedge P_x$$

אם המערכת לניהול בסיס נתונים מאפשרת למשתמש לבצע שאילתות ולהוסיף רשומות, קל ופשוט לשלוף מידע חסוי אודות פרט מסוים,

שניתן לזיהוי וודאי בעזרת קבוצת התכונות C. נניח שהמערכת אינה מאפשרת לבודד משתמש, מכיוון שהותקנה הגנה שאינה מאפשרת לשלוף קבוצת שאילתה קטנה. בהתקפה במקרה זה תהיה הוספה של רשומות מדומות לבסיס הנתונים. רשומות מדומות אלו מכילות את קבוצת התכונות C. אם מספר הרשומות שנוספו הוא לפחות (N_{min} - 1), אפשר לחשוף את המידע החסוי באופן שתואר למעלה.

עוקב (traker) הוא שיטת התקפה נוספת שמתגברת על התקן ההגנה הקובע את גודל קבוצת השאילתה. עוקב הוא ביטוי חיצוני המפיק תשובה, שביחד עם תשובות אחרות מאפשרת למצוא מענה לשאילתה שלא ניתן לקבל עליה תשובה. לדוגמה, אם ניתן לזהות פרט מסוים בעזרת קבוצת המאפיינים C, אפשר לייצג זאת גם כך:

$$C = C_1 \wedge C_2$$

אם המערכת תגיב לשאילתות של (C_1) ושל ($C_1 \wedge \overline{C_2}$), אז נכנה את ($C_1 \wedge \overline{C_2}$) "העוקב של הפרט" (שלורר, 1975).

הדוגמה שבטבלה 3.3 מציגה פרטים חסויים על משכורות של בעלי תפקידים בכירים בעיתון. עבריין רוצה לחשוף את המשכורת של הכתבת גב' B. אפשר להשיג זאת אם נגדיר C_1 = כתב/ת ו-C_2 = נקבה, העוקב יהיה:

(קרא מימין:) (כתב $\wedge$ לא נקבה) = (כתב וגם זכר)

שאלה: כמה כתבים יש?
תשובה: 4
שאלה: כמה כתבים הם זכרים?
תשובה: 3

שתי שאלות אלו מאשרות את העובדה שישנה רק כתבת אחת, גב' B.

שאלה: מהו הסכום הכולל ששולם לכתבים?
תשובה: 68,000 שקל
שאלה: מהו הסכום הכולל ששולם לכתבים הזכרים?
תשובה: 48,000 שקל.

המסקנה מתשובות אלו היא שהתשלום לגב' B היא 20,000 שקל.

אפשר לחשוב שקשה מאוד לחשוף חלק גדול מבסיס הנתונים בגלל הצורך לדעת מאפיינים מזהים של אנשים, כדי לבנות להם עוקבים. אין זה נכון. הוכח (שלורר, 1979) שקל מאד למצוא עוקבים, גם בעזרת שאילתה אחת או שתיים.

טבלה 3.3 בסיס נתונים המאחסן משכורות

שם	מקצוע	זכר	נקבה	תשלומים
מר A	עורך	כן		25,000 ש'
גב' B	כתב		כן	20,000
מר C	כתב	כן		19,000
מר D	כתב	כן		16,000
מר E	עיתונאי	כן		16,000
גב' F	עיתונאי		כן	17,000
גב' G	עיתונאי		כן	17,000
מר H	מהנדס	כן		15,000
גב' I	מהנדס		כן	14,000
מר J	כתב	כן		13,000

התקפה בשיטת העוקב מנצלת את העובדה שקבוצות שאילתות חופפות זו את זו. חפיפת זו מאפשרת גם לתקוף את בסיס הנתונים בעזרת משוואות סימולטניות (simultaneous equations). אם בסיס הנתונים מבוסס על קבוצה של מספרים, לדוגמה X1, X2, X3 ו-X4, ואפשר לבצע שאילתות על הסכום של כל תת קבוצה, אפשר לקבל את סדרת השאילתות והתשובות הבאה:

שאילתה 1: (X1 + X2 + X3) תשובה: A1
שאילתה 2: (X1 + X2 + X4) תשובה: A2
שאילתה 3: (X1 + X3 + X4) תשובה: A3
שאילתה 4: (X2 + X3 + X4) תשובה: A4

פתרון ארבע המשוואות יוביל למציאת כל אחד מבין המספרים שמרכיבים אותן. לדוגמה:

$$X_3 = (A_1 + A_3 + A_4 - 2 \times A_2) / 3$$

אחת הדרכים להגן על בסיס נתונים מפני התקפה מסוג זה היא להבטיח שחפיפה קטנה בין קבוצות של שאילתות. בהעדר חפיפה, תאבד התקפה מסוג משוואות סימולטניות כל משמעות.

3.5.4 מנגנוני בקרת ההיקש והקשיים ביישומם

מנגנוני ההגנה כוללים:

(1) בקרות על גודל קבוצת שאילתה.
(2) בקרות על החפיפה בין קבוצות שאילתות.
(3) בקרות שמעוותות את התשובות, כמו לעיגול תוצאות או אספקת תשובות מזויפות.

בדוגמאות שהובאו בסעיף 3.5.3, רואים שהסיכון לבסיס נתונים סטטיסטי נובע מקבוצת שאילתה קטנה ומקבוצת שאילתה גדולה. קל להתקין מנגנון שיבקר את גודל קבוצת השאילתה, ותועלתו רבה. למרבה הצער המנגנון אינו מספק, כי אפשר לעקוף אותו בעזרת עוקב. מנגנוני בקרה שפועלים על גודל קבוצת השאילתה מקשים על עבודתו של פורץ פוטנציאלי. כדי למנוע התקפות שמנצלות את החפיפה בין קבוצות שאילתות, יש למנוע תשובות לשאילתות שהחפיפה בין קבוצות השאילתות שלהן גדולה מדי. באכיפת מנגנון כזה, אפשר למנוע תשובות גם לשאילתות אמיתיות ומועילות. לכן, בקרת חפיפה איננה מעשית, בדרך כלל, כי היא מגבילה שימוש בבסיס הנתונים.

המנגנונים שנדונו מגבילים נתונים סטטיסטיים שיכולים להוביל לחשיפה, אבל הם מספקים מידע מדויק. כמה מהמנגנונים אינם מספקים מידע מדויק, אך הם מנסים למנוע חשיפה בעזרת הוספת רעש לתשובות, או עיוות של הערכים שנמצאים בבסיס הנתונים. עיגול מספרים (rounding) הוא טכניקה שמטפלת בנתונים סטטיסטיים בטרם יועברו למשתמש הקצה (אצ'וגבו וצ'ין, 1979). טכניקה זו יעילה רק בבסיסי נתונים סטטיים. כלומר, רק במצבים שבהם המשתמש אינו יכול להוסיף, או לבטל, רשומות ולכן היישום של שיטה זו מוגבל. הכנסת טעויות (error inoculation) (בק, 1979) מעוות את הערכים בבסיס הנתונים. אין זה רצוי כאשר היישומים אמורים להשתמש במידע מדויק ומפורט. דגימה היא שיטה נוספת שאינה מספקת תשובות אמיתיות, אלא כאלו שמבוססות רק על חלק מבסיס הנתונים. הסיכוי לפגוע בבסיס הנתונים קטן, כי לעבריין אין אפשרות לבחור את קבוצת הרשומות.

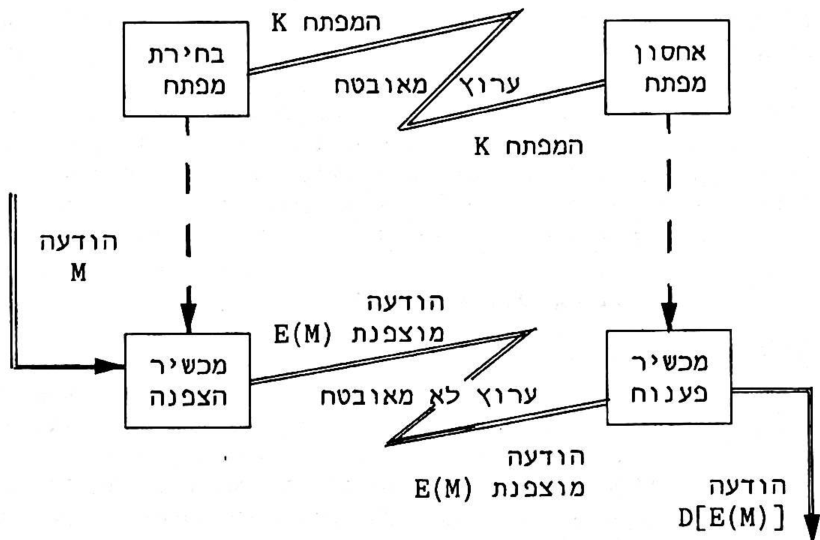
מנגנוני השאילתות בבסיסי נתונים רבים מספקים מידע מעל למה שמשתמשים רגילים של בסיס הנתונים יכולים לשער. קיימות הוכחות שהמנגנונים, שתוארו לעיל, אינם מספקים הגנה מספקת במקרים רבים. לכן, לעתים קרובות יש להוסיף לבקרות ההיקש ניטור איומים (treat monitoring) (הופמן, 1977), שיבצע מעקב אחר שאילתות, כדי לגלות פרקי זמן שבהם פעילות רבה, וניסיונות שליפה באמצעות שאילתות דומות. ניטור משמש כאמצעי מניעה פסיכולוגי.

3.6 הצפנה

3.6.1 העקרונות הבסיסיים של הצפנה ומטרותיה

במצבים מסוימים נמצא שבקרות כניסה, זרימה והיקש אינן מספיקות כדי להבטיח הגנה נאותה למידע. בנסיבות כאלו, יש להשתמש בהצפנה כדי שמידע סודי, אם יפול בידיים הלא נכונות יהיה חסר ערך, מכיון שמשמעותו תשאר סמויה. הצפנה, המדע של הכתיבה הסודית, משמש אנשים ומדינות מאות שנים, כדי למנוע חדירה למידע שבמסמכים (קאהן, 1967). מערכת הצפנה מתוארת בתרשים 3.7. הודעה רגילה M עוברת תהליך של שינוי והופכת להודעה מוצפנת E(M). תהליך זה נקרא הצפנה.

תהליך ההצפנה (או הפענוח) מתבסס על אלגוריתם ומפתח הצפנה. האלגוריתם נשלט במפתח K. ההודעה המעורבלת משודרת בערוץ לא מאובטח, והמקבל משחזר אותה בשיטת פענוח; כלומר, M = D[E(M)] . מערכת הצפנה סימטרית משתמשת באותו מפתח להצפנה ופענוח, בניגוד למערכת הצפנה אסימטרית, שמשתמשת במפתחות שונים בקצוות השונים של ערוץ התקשורת (סימונס, 1979). הצפנה סימטרית היא גישה קונבנציונלית, שרמת האבטחה שהיא מספקת תלויה בסודיות המפתח. לכן משודר המפתח בערוץ מאובטח. ההודעה המעורבלת E(M) משודרת בערוץ לא מאובטח.



תרשים 3.7 מערכת הצפנה (cryptosystem)

מנגנוני הצפנה מספקים הגנה בדרכים שונות, כולל הגנה של:

(1) סיסמאות.
(2) מידע בבסיס נתונים - במקרה (A) שהיתה אליו גישה של אנשים שאינם מורשים, או במקרה (B) שבו נגנב דיסק המכיל בסיס נתונים.
(3) מידע במעבר דרך ערוץ תקשורת - בפני ציתות או התחברות לא חוקית לקו.

3.6.2 מערכות הצפנה קלסיות

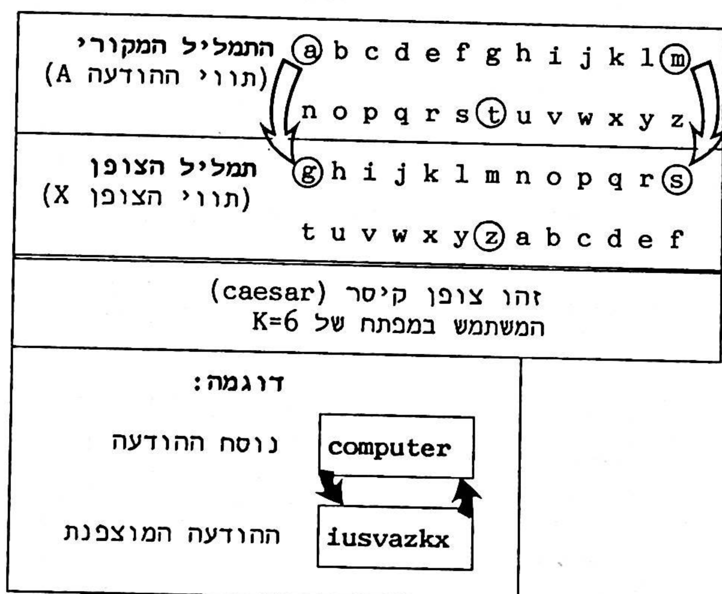
קיימים שני סוגים בסיסיים של מערכות הצפנה. הראשונה משתמשת בהחלפת אותיות (substitution) והשניה משתמשת בהתמרות (transposition), או בהחלפת מקומות. בנוסף לכך, ניתן להשתמש בטרנספורמציות מעורבות שמשלבות החלפת אותיות ובהתמרות. טרנספורמציות אלו מוכרות בשם "טרנספורמציות כפולות" (product tranformation). שני סוגי הטרנספורמציות הבסיסיות אינם מספיקים למערכת הצפנה, מכיון שמומחה לפענוח יכול לשבור אותן בקלות בעזרת מחשב. טרנספורמציות כפולות מתאימות במיוחד לעידן המחשבים.

בטרנספורמציות של החלפת אותיות מוציאים תווים מההודעה ומחליפים אותם בתווים הנלקחים מצופן. טרנספורמציה פשוטה המשתמשת בהחלפת אותיות, המבוססת על שפה אחת, מתוארת בתרשים 3.8. בהחלפת אותיות זו נבנה צופן X שיתאים לאותיות האפשריות בהודעה A. כלומר, לכל תו ב-A, תו אחד ויחיד המתאים לו ב-X. קל לשבור סוג זה של מערכת הצפנה בגלל מאפייני שפה (שנון, 1951). לתווים התואמים בהודעה המוצפנת תהיה תדירות מופע יחסית הזהה לזו של התווים בהודעה המקורית, כמו האות e, שהיא האות השכיחה ביותר באנגלית. ניתן לשפר גישה זו על ידי החלפה שמתבססת על מספר שפות (קאהן, 1967) שתחליף את המאפיינים הסטטיסטיים של השפה היחידה. מערכת הפועלת לפי שיטה זו, כוללת n סוגי אותיות:

$$x_1, x_2, x_3, x_4, \ldots, x_n$$

ההחלפה הראשונה היא מ-x_1; ההחלפה השניה היא מ-x_2 וכן הלאה, עד שהתו n יוחלף עם תו מ-x_n. ההצפנה ממשיכה עד החזרה לתו x_1.

ניתן להשתמש בהחלפות המבוססות על שפה אחת, או על כמה שפות, ביחד עם החלפות חד-תוויות, שבהן מוחלפים תווים בודדים. אפשר לשלב זאת עם החלפות רב-תוויות, שבהן קבוצה של תווים מוחלפת על ידי קבוצה אחרת בעלת מספר תווים זהה.



תרשים 3.8 טרנספורמציה מסוג החלפת אותיות

3.6.3 תקן להצפנת נתונים - DES

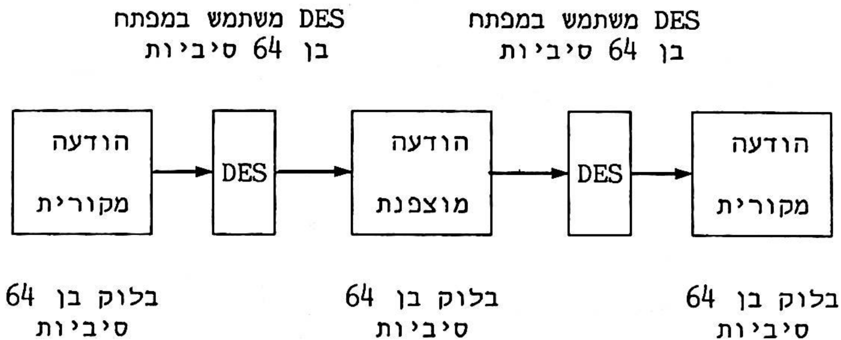
הצורך בתקן להצפנת מידע ממשלתי, שאינו נושא אופי צבאי, התעורר בארצות הברית באמצע שנות ה-70. שיטות ההצפנה התפתחו מאז שנות ה-40 רק בתחומי הצבא ובתחומי הבטחון הלאומי, בעוד שבמוסדות ממשלתיים לא מסווגים לא התעורר עניין בנושא זה. לאחר ארבע שנים של בחינה מדוקדקת, אישר מכון התקנים האמריקאי (NBS) טרנספורמציית הצפנה ספציפית - ה-DES (Data Encryption Standard) שהוגדרה כתקן (סטנדרט) להצפנת נתונים (FIPS 46 ,1977).

התקן משתמש בטרנספורמציה כפולה של התמרות, החלפות ופעולות לא ליניאריות. ההודעה שמיועדת להצפנה מחולקת לבלוקים בני 64 סיביות. כל בלוק של ההודעה עובר 16 איטרציות שלאחריהן מתקבל בלוק מוצפן בן 64 סיביות. המפתח בן 56 הסיביות, הוא תוצר של מפתח בן 64 סיביות, ש-8 מהן משמשות לבדיקת זוגיות (parity bits). בתקן DES שמתואר בתרשים 3.9, משמש אותו אלגוריתם להצפנה ולפענוח של כל בלוק מוצפן. כלומר, פעם אחת הופכים את ההודעה המקורית לתמליל מוצפן ואחר כך, מחזירים אותה לקדמותה.

תקן DES תומך במטרות הבאות:

(1) הגנת סיסמאות.
(2) הצפנה מקצה לקצה, כמתואר בתרשים 3.10.
(3) הצפנה של קבצים שמאוחסנים על אמצעים נתיקים.

אפשר ליישם טרנספורמציות DES גם בחומרה. בארצות הברית אפשר ניתן להשיג מעגלים משולבים המכילים את התקן הזה.



תרשים 3.9 DES

3.6.4 עמידותו של DES בפני התקפה

בהנחה שהמפתח אינו ידוע, המומחה לפענוח יכול לנקוט בשלוש שיטות של תקיפה או פיצוח הקוד:

(1) תקיפה שמתבססת רק על ההודעה המוצפנת - שבה מחזיק המומחה לפענוח העתקים של הודעות מוצפנות, אך אין הוא מכיר את ההודעות המקוריות.
(2) תקיפה שמתבססת על הודעה מקורית - שבה מחזיק המומחה לפענוח בהודעה המוצפנת ובהודעה המקורית שמתאימה לה.
(3) תקיפה שמתבססת על הודעה מקורית נבחרת - שבה מחזיק המומחה לפענוח הודעה מקורית נבחרת וביכולתו להשיג את ההודעה המוצפנת המתאימה לה.

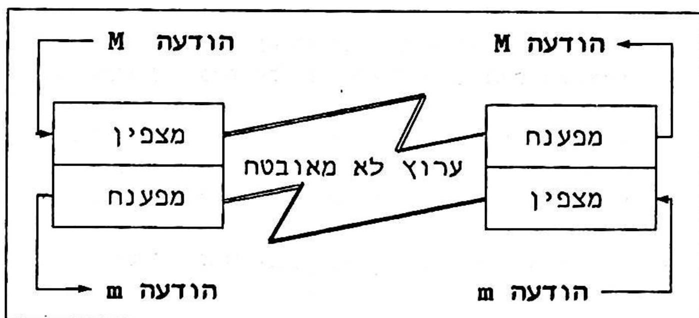
בדקו את יכולתו של DES לעמוד בפני התקפה שמתבססת על הודעה מקורית ואת כושר עמידתו בפני פיצוח. שבירת הצופן מחייבת את המומחה לפענוח לנסות 2^{56} או 7.2×10^{16} מפתחות אפשריים עם ההודעה המקורית, כדי לחשוף את המפתח שהפיק את הגרסה המוצפנת של ההודעה. משך הזמן הנדרש לבדיקת כל מפתח הוא אלפית השניה ולכן, ניסוי שיטתי של כל המפתחות נמשך 7.2×10^{10} שניות.

דיפי והלמן (1977) טענו שמבחינה כלכלית וטכנית, כדאי לבנות מחשב מקבילי עם מיליון שבבים כדי להשלים את החיפוש במשך 7.2×10^4 שניות, או 20 שעות. מחירו של מחשב כזה היה אמור להיות 20 מיליון דולר. דיפי והלמן הסיקו מכך שמפתח בן 56 סיביות קצר מדי, ומפתח בן 128 סיביות ימנע למעשה את שבירת DES. המפתחים של DES ב-יבמ ממשיכים לדבוק בגרסה האומרת, שאפילו מפתח הצפנה בן 56 סיביות אינו הנקודה החלשה במערך האבטחה.

הפרטים המלאים של טרנספורמציות DES פורסמו ברבים ולכן, האבטחה של מערכת ההצפנה תלויה במידת האבטחה של המפתחות. בעת הטיפול במפתחות יש להתחשב בשיקולים הבאים:

(1) אחסון - יש להצפין את המפתחות.
(2) הפצה - זו יכולה להתבצע בעזרת שליח מיוחד, באמצעות הדואר, או דרך רשת תקשורת מחשבים.
(3) אקראיות - יש להפיק מפתחות בעזרת מספרים אקראיים.

מערכת הצפנה סימטרית, כמו DES, הופכת את הבעיה של הגנת הנתונים לבעיה של הגנת המפתחות בזמן השימוש או במהלך הפצתם.



תרשים 3.10 הצפנה מקצה לקצה

3.6.5 הצפנה בעזרת מפתח ציבורי

הצפנה בעזרת מפתח ציבורי שונה מהגישות המסורתיות, כי היא אסימטרית, ומכיוון שמפתח ההצפנה Ke מפורסם ברבים (דיפי והלמן, 1976). מפתח ההצפנה Ke ומפתח הפענוח Kd שונים זה מזה, אך בשניהם חייבים להתקיים התנאים הבאים:

(1) $M = D[E(M)]$.
(2) יש למנוע אפשרות של חישוב Kd מתוך Ke.

מערכת ההצפנה פועלת באופן הבא:

(1) ארגון או אדם פרטי מפיק זוג מפתחות תואמים (Ke ו-Kd).
(2) מפתח ההצפנה Ke מתפרסם במדריך.
(3) כל מי שרוצה לשלוח הודעה M לאותו ארגון, מחפש במדריך את מפתח Ke ושולח הודעה מוצפנת E(M).
(4) עבריין המיירט את ההודעה, מחזיק בהודעה המוצפנת E(M) ביחד עם מפתח ההצפנה Ke, אבל עליו לחשב את Kd מתוך Ke.

פעולת ההצפנה חייבת להתבצע בכיוון אחד, בפשטות ובאופן שאינו ניתן לשחזור. מתכנן זוג המפתחות התואמים מחזיק במידע נוסף, שמשמש אותו ליצירת מפתח הפענוח Kd. אפשר לכנות מידע סודי זה "שביל הזהב" (trapdoor), כי הוא מאפשר פתרון למצב שנראה בלתי ניתן לפתרון.

3.6.6 המפתח הציבורי של ריווסט, שמיר ואדלמן

אחד היישומים הראשונים והידועים של המפתח הציבורי מבוסס על הקושי לפרק מספר שלם וגדול לגורמיו הראשוניים (ריווסט, 1978). להלן, המאפיינים העיקריים של יישום זה:

(1) ההודעה M - המוצפנת, המפתחות וטרנספורמציות הפענוח וההצפנה מיוצגים על ידי מספרים שלמים וחיוביים.

(2) מפתח ההצפנה Ke ומפתח הפענוח Kd נבחרים באופן הבא:

א. בוחרים בצורה אקראית שני מספרים ראשוניים גדולים: p ו-q שבכל אחד מהם יותר מ-100 ספרות.

ב. מחשבים שתי מכפלות:
$$n = pq$$
$$r = (p-1)(q-1)$$

ג. בוחרים, באופן אקראי, מספר שלם e, שמקיים את שני התנאים:
ל-e אין גורם משותף עם r. $e < r$

ד. מחשבים את המספר השלם d בעזרת המשוואה הבאה:
$$ed = 1 \bmod r = 1 \bmod (p-1)(q-1)$$

ה. יוצרים את מפתח הפענוח, המפתח הסודי, כ-(d,n) ואת מפתח ההצפנה כ-(e,n).

(3) כוחה של שיטה זו נובע מהקושי למצוא את d, כי הדבר דורש פירוק לגורמים של n, כאשר n הוא מספר בן 200 ספרות.

(4) ההודעה M הופכת להודעה סודית C בעזרת הנוסחה:

$$C = M^e \bmod n$$

(5) ההודעה המקורית משוחזרת מההודעה המוצפנת בעזרת הנוסחה

$$C^d \bmod n = M$$

דוגמה:

נתון מקרה פשוט, שבו:

שלב 2a

שני המספרים הראשוניים שנבחרו:

p=7 ,q=11

שלב 2b

מחשבים את שני המספרים, n ו-r:

$n = pq = 7 \times 11 = 77$

$r = (p - 1)(q - 1) = 6 \times 10 = 60$

שלב 2c

בוחרים מספר שלם e, שמקיים את התנאים:

$e < r$

ל-e אין גורם משותף עם r

בחרנו $e = 37$

שלב 2d

מחשבים את המספר השלם d בעזרת המשוואה:

$ed = 1 \bmod r = 1 \bmod (p - 1)(q - 1)$

$37d = 1 \bmod 60$

$d = 13$

שלב 2e

מפתח הפענוח, המפתח הסודי, הוא (13,77)

מפתח ההצפנה, המפתח הציבורי, הוא (37,77)

דוגמה זו אינה ריאלית, אך היא מציגה בפשטות את תהליך קריאת המפתחות. קיימים כמובן צירופים נוספים של d ו-e, הנותנים את צמד הערכים:

[r = 60-ו n = 77]

לדוגמה, אם e=11, ניתן לחשב את הערך המתאים של d.

בשיטת טרנספורמציה זו דרך הפתרון הינה על ידי פירוק של n לגורמים. לא הוכח שפירוק לגורמים קשה מיסודו אך המתימטיקאים לא הצליחו למצוא תהליך פירוק מהיר. שני מתימטיקאים אירופיים פיתחו שיטה מהירה שבעזרתה ניתן לקבוע אם מספר הוא ראשוני (סאליבן, 1982). מעניין יהיה לבדוק אם שיטה זו תפגע בשיטת הטרנספורמציה של ריווסט המבוססת על המפתח הציבורי.

3.6.7 חתימות דיגיטליות

הודעות הנשלחות דרך רשתות תקשורת עשויות לסייע בניהול משאבים פיננסיים וכד'. מסלקות בין בנקאיות ומערכות אלקטרוניות להעברת כספים (EFT) ישמשו דוגמאות לכך. במצבים כאלה חשוב להשתמש בשיטות שיוכיחו את האותנטיות והאמיתות של ההודעה המתקבלת, בדומה למערכות ידניות מסורתיות שבהן מאמתות חתימות את המסמכים. אפשר ליישם חתימות דיגיטליות בעזרת מערכת הצפנה שמבוססת על המפתח הציבורי, בתנאי שמערכת ההצפנה נושאת את התכונה E[D(M)]=M, כלומר - הפענוח קודם להצפנה. תהליך זה מתואר בתרשים 3.11. השולח A, שרוצה ליצור חתימה, משתמש לצורך ההצפנה בהודעה M עם המפתח הסודי Kd, כדי להפוך הודעה מעורבלת $D_A(M)$. המקבל B, שרוצה לבדוק את מקור ההודעה, צריך להשתמש במפתח הציבורי Ke של השולח A בכדי לפענח את ההודעה, רק אז $E_A[D_A(M)]=M$. אפשר להוסיף לשיטה זו מרכיב סודיות, אם השולח A ישתמש במפתח ההצפנה E_B של המקבל B, לאחר התהליך שתואר לעיל. גם שיטה זו מתוארת בתרשים 3.11.

השולח A רוצה לשלוח חתימה דיגיטלית			המקבל B רוצה להיות בטוח שההודעה אכן הגיעה מ-A		
הודעה	תהליך פענוח של A	הודעה מעורבלת	תהליך הצפנה של A	הודעה	(A)
M	$D_A(M)$	$D_A(M)$	$E_A(D_A(M))$	M	(A)
הודעה	1) תהליך פענוח של A, ואז 2) תהליך הצפנה של B	הודעה מעורבלת	3) תהליך פענוח של B ואז 4) תהליך הצפנה של A	הודעה	(B)
M	1. $D_A(M)$ 2. $E_B(D_A(M))$	$E_B(D_A(M))$	3. $D_B(E_B(D_A(M))$ $=D_A(M)$ 4. $E_A(D_A(M))$	M	(B)

תרשים 3.11 חתימות דיגיטליות
(a) עם מרכיב סודיות, (b) ללא מרכיב סודיות

3.7 מסקנות

אפשר להגן על הנתונים בעזרת ארבעה סוגי בקרות: בקרות כניסה, בקרות זרימת נתונים, בקרות היקש ושיטות הצפנה. כשהן מופעלות יחד הן מפחיתות, אך אינן מסירות, את סכנת הפגיעה בנתונים, כי לכולן מגבלות תיאורטיות ומעשיות. עד שאופנים אחרים של אימות וזיהוי חד משמעי יהפכו לכדאיים מבחינה כלכלית, ישמשו הסיסמאות מנגנון בקרת כניסה למערכות מחשב. אפשר להשיג בקרת כניסה אידיאלית בעזרת העיקרון של כמות הרשאות קטנה ככל האפשר, שניתן ליישם אותן במחיר סביר. עם זאת, קשה להוכיח שהמערכת אכן פועלת בהתאם למפרט של בקרת הכניסה ושההרשאות ממלאות אחר הדרישות של בעלי המידע.

בקרות זרימה משתמשות בנתונים ובמערכות קלט של תכניות, כדי לקיים את מסלולי ההפצה של הנתונים. קיים חשש שמגנונים המשתמשים ברמות אבטחה יסווגו את המידע ברמה גדולה מדי. יש לזכור שקשה להסדיר את זרימת המידע בערוצים סמויים.

אם למשתמש אין הרשאה לגישה ישירה למידע חסוי בבסיס נתונים הוא יכול להגיע למידע על ידי התאמת תשובות לשאילתות, שאינן מזיקות לכאורה. בקרות היקש עשויות להקטין את הדליפה, אבל בקרות הדוקות מדי אינן מאפשרות לנצל את בסיס הנתונים ביעילות. כתוצאה מכך, מנגנוני בקרת זרימה מאפשרים למידע סודי לחמוק מבסיס הנתונים ולכן הם מותקנים בעיקר כדי להקשות על המלאכה של עבריין פוטנציאלי.

הצפנה מספקת הגנה כאשר בקרות אחרות אינן מספיקות. רמת האבטחה שמספקת מערכת הצפנה סימטרית, תלויה בהפצה בטוחה של המפתחות. למרות שהצפנה המבוססת על המפתח הציבורי מסירה את הקושי שבחלוקת מפתחות, קיים, בכל זאת, צורך להגן על המפתח הסודי המרכזי.

ישנו הבדל גדול בין סוג ההגנה שמתאים למעבדה לבין סוג ההגנה שנדרש במערכות מסחריות רבות. בתוך מערכת המידע הכוללת, משמשת אבטחה פנימית של הנתונים במחשב רק מרכיב אחד. רוב הפגיעות באבטחה קשורות לאבטחה חיצונית. אבטחת נתונים היא מהמרכיבים היותר נשלטים של אבטחה מערכת המידע.

שאלות

3.1 לעתים קרובות טוענים שעדיף להעניק למשתמשים שליטה בעבודתם. מדוע יעיל יותר להרשות להם לבחור את הסיסמה שלהם, מלהשתמש בסיסמאות הנבחרות בצורה אקראית על ידי המחשב?

3.2 הסבר מדוע כל אופני הצגת הסיסמאות אינם בטוחים.

3.3 חשב את משך השבירה של מערכת סיסמאות, כאשר מתבצע חיפוש שיטתי. קצב ההקלדה הוא 60 תווים לדקה; מערכת התווים היא בת 26 תווים; אורך הסיסמה 6 תווים ומספר התווים שיש להקיש בכל תהליך הכניסה הוא 12.

3.4 תכנן אורך סיסמה לפי הנתונים הבאים: ניתן להשתמש בכל אחד מ-26 תווים; הסיכוי שיגלו את הסיסמה, בהתקפה של חיפוש שיטתי במשך 3 חודשים, הוא 0.001; קצב הקלדת הנתונים הוא 60 תווים לדקה; בתהליך הכניסה יש להקיש 12 תווים.

3.5 רשת תקשורת משתמשת בסיסמאות אימות בשני הכיוונים. הסבר מדוע ניתן בכל זאת ליירט את הנתונים ומדוע מערכת סיסמאות זו אינה מספיקה.

3.6 מהם היתרונות והחסרונות של:

(א) אלגוריתם לאימות ולזיהוי המשתמש, בהשוואה לנוהל פשוט של הכנסת סיסמאות.

(ב) נוהל של סיסמה חד פעמית, בהשוואה לנוהל פשוט להכנסת סיסמאות.

3.7 בסיסי נתונים פגיעים להתקפה מסוג של היקש לוגי. כיצד יעזור ניטור איומים לשיפור האבטחה?

3.8 בהנחה שמידע אישי המתייחס אליך מוחזק במחשב המוסד שבו אתה לומד, ציין את התכונות שיבודדו אותך בבסיס נתונים.

3.9 חבר שלך מתבקש לספק מידע אישי שיישמר בבסיס נתונים סטטיסטי גדול השייך לממשלה. הוא מוכן לשתף פעולה למרות שהוא לא חייב בכך, אבל הוא מודאג, מכיוון שנתונים מסוימים יכולים להביך אותו אם יתפרסמו ברבים.

(א) אילו בטחונות יש לתת לחבר שלך אם מעוניינים בשיתוף פעולה מצידו?

(ב) אם אתה הוא מתכנן המערכת, האם תוכל לתכנן את הבטחונות האלה? איזה תחום יהיה הקשה ביותר לתכנון?

3.10 אותו חבר מחזיק בתכונות P1, P2, P3...P12 שמאפיינות אותו במיוחד. כתוב משוואות שתייצגנה שתי דרכים המאפשרות לגלות אם לחברך מחזיק בתכונה P9.

3.11 נוהג נפוץ הוא לשנות סיסמאות בפרקי זמן קבועים. למשל, באוניברסיטאות, בתחילתה של כל שנה אקדמית, או במרכזי מחשב עסקיים, בסוף כל חודש או רבעון. הסבר מהן

החסרונות של שיטה זו והצע דרכים לשיפורה.

3.12 הסבר מהם ההבדלים בין רשימת הרשאות לבין מדיניות אבטחה בעלת מספר רמות סיווג.

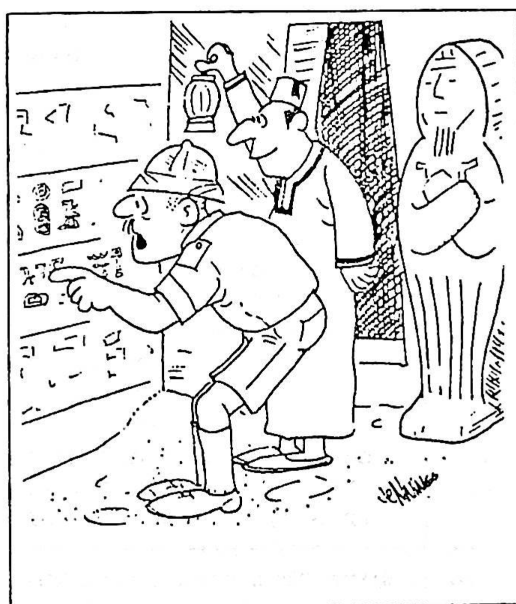
3.13 רשימה של כל הסיסמאות נשמרת במערכת ההפעלה. משתמש שמצליח לקרוא את הרשימה, שובר, למעשה, את ההגנה שמספקות הסיסמאות. הצע שיטה שתעזור למנוע סיכון זה.

3.14 הסבר מדוע מערכת הצפנה המבוססת על החלפה פשוטה אינה מספיק חזקה. האם קיימות נסיבות שבהן תשתמש במערכת כזו?

3.15 בקר מספר פעמים במרכז המחשבים שאתה קשור אליו והכן דוח שיתבסס על קריאת מדריכים לתוכנה ולחומרה ועל תחקור צוות התפעול הבכיר במתקן. הדוח צריך לכסות את הנושאים הבאים:

(א) אמצעי אבטחה שהותקנו על ידי יצרני חומרה ותוכנה.
(ב) סיסמאות ואימות המשתמשים.
(ג) בקרת היקש במערכות לניהול בסיס נתונים.
(ד) אפשרויות הצפנה.

הדוח צריך להתפרש על עמוד עד שלושה עמודים ועליו לשקף את ממצאיך ומסקנותיך. יש לצרף נספחים שמתארים במפורט את תוצאות החקירות שלך: נספח אחד לכל נושא שנרשם לעיל (משימה קבוצתית).



כניסה ללא הרשאה

פרק 4

התפקיד שממלאים מרכיבי מערכת המחשב באבטחה

בפרק הקודם דנו בטכניקות בקרה שמשמשות באבטחת נתונים: בקרת כניסה, בקרת זרימה, בקרת ההיקש ובקרה באמצעות הצפנה. בפרק זה נדון בחומרה, במערכת ההפעלה, בתקשורת ובמסופים ונראה כיצד מיושמות טכניקות הבקרה במערכות אלו. האבטחה של מערכות מקוונות תלויה בתוכנה יישומית (שבתכנונה נדון בפרק 6). תוכנה יישומית למערכות מקוונות דורשת, כמו תוכנה יישומית אחרת, סביבה בטוחה, שבה תוכל לפעול. את הסביבה הבטוחה מספקים אמצעי האבטחה הנמצאים בתוך המחשב ובתוך שאר המרכיבים של מערכת המחשב. אפשר לתכנן את החומרה כדי שתבדוק בעצמה את פעולתה ואפשר לשלב בדיקות רבות ושונות לגילוי טעויות. אלו בקרות מקיפות ויעילות.

טבלה 4.1 איומים הקשורים לחומרה, לתקשורת ולמערכת ההפעלה

סוג האיום	האיום	האובדן
לא מכוון לא מכוון מכוון	תקלה בחומרה טעויות של מפעילים התקפה פיסית או חבלה	זמינות של שירותים
לא מכוון לא מכוון מכוון	תכנון לקוי של מישק אדם-מחשב טעויות של מפעילים שינוי ללא הרשאה של נתונים	שלימות נתונים
מכוון	שינוי ללא הרשאה של טבלת הרשאות	שלימות המערכת
מכוון מכוון	כניסה ללא הרשאה של אנשים המתחזים למשתמשים מורשים התקפה על התקשורת (ציתות)	סודיות
מכוון	פורץ מחוכם גורם תקלה בחומרה כדי להסוות התקפה אמיתית	סודיות ושלימות נתונים

לפני כעשר שנים, לא ענו מערכות ההפעלה על כל דרישות האבטחה, אבל מצב זה השתנה בצורה דרמטית. עבריין בעל ידע יכול עדיין לעקוף את בקרות מערכת ההפעלה, אך רמת האבטחה הקיימת במערכות הפעלה רגילות המסופקות על ידי יצרני מחשב, גבוהה מזו שקיימת בחומרה. אמצעי האבטחה המסופקים על ידי החומרה והתוכנה יכולים להוות בסיס טוב, גם אם לא מושלם, שאפשר לבנות עליו מערכות מידע. דבר זה נכון לגבי מערכות ריכוזיות הנמצאות באתר אחד. לצערנו, המצב פחות טוב במערכות המותקנות בכמה אתרים, במערכות מקוונות ובעיבוד מבוזר של נתונים. המורכבות מסבכת את הבעיות של פעולה באתר אחד וכפי שמתואר בטבלה 4.1, הדבר עלול לגרום לטעויות, להשמטות ועוד.

4.1 חומרה

המחשב הוא מכשיר אלקטרוני מורכב, שמחובר להתקני קלט/פלט אלקטרוניים ואלקטרו-מכניים. האיומים שאליהם הוא חשוף:

(1) תקלה באחד ממרכיבי המכונה.
(2) טעות של מפעיל.
(3) התקפה פיסית על המחשב.

תקלות במכונה שונות מטעויות של מפעיל ומהתקפה פיסית, בכך שאי אפשר לראותן. לכן נדרשים מנגנוני אבטחה מיוחדים. אם מתרחשת תקלה במרכיבי החומרה של מערכת המידע, קיימת סכנת פגיעה במנגנוני האבטחה של החומרה, ובמנגנוני אבטחה שנמצאים בכל מקום אחר במערכת המידע. לדוגמה, קיימת אפשרות שתקלה בחומרה תגרום גם לתקלה בתוכנה.

מרכיבי החומרה העיקריים במערכת המחשב: הזיכרון ראשי, יחידת העיבוד המרכזית (יע"מ), הזיכרון המשני והציוד ההיקפי. מטרת אבטחת החומרה היא להכניס אמצעי הגנה למרכיבים אלה ולתקן אותם כך שהמחשב יוכל לבדוק את פעולותיו, לגלות שגיאות ולתכן אותן, היכן שאפשר. מספר אמצעי ההגנה והתחכום של המנגנונים משתנה ממכונה למכונה. השוני מושפע מהגורמים הבאים:

* הצרכים של מערכת המידע והמשתמשים, כפי שניצפו על ידי המתכנן.
* המחיר.
* היכולת של המתכנן לעמוד בדרישות.

בנוסף להשפעה על עלויות, פוגעים אמצעי האבטחה בביצועי המחשב. מנגנוני אבטחה בחומרה נחשבים לגורמי תקורה במערכת. בעבר ניסו יצרני מחשבים לצמצם עומס זה, ככל האפשר.

היעד הבסיסי של אבטחת חומרה הינו הגנה על המידע המיוצג בחומרה ונשמר כתוכנות וכנתונים. מכיוון שיחידות הזיכרון ואמצעי האחסון הם למעשה מאגרים של תוכניות ונתונים, נדרשים מנגנוני האבטחה לדברים הבאים:

* הסדרה של העברת המידע בין המאגרים, כפי שתואר בפרק 3.
* פיקוח על העברת הנתונים בין המאגרים.
* יצירת מאגרים מוגנים.

יעדים אלה מושגים בעזרת אמצעים המאפשרים הגנת זיכרון ומצבי עיבוד מרובים, שנדון בהם בסעיף 4.1.2. אולם, כאשר המתכנן של אבטחת החומרה עומד ליישם את המנגנונים האלה הוא נתקל בבעיה של בחירת גודלו של הרכיב שבו עליו להתקין את ההגנה. לדוגמה, אפשר להרכיב מנגנונים להגנת זיכרון ברמת המלה או ברמת הבלוק וכידוע, הגנה ברמת המלה יעילה יותר, אך יקרה יותר. עובדה זו מדגישה שוב את הבעיה הניצבת בפני המתכנן, כלומר איזון בין רמת המחיר לרמת האבטחה.

4.1.1 הגנת זיכרון

מרחב כתובות הוא זיכרון שמשמש את המערכת ואת תוכניות היישום. הוא מאפשר לתוכניות שרצות במחשב לפנות למקומות שונים בשטח הזכרון שמוקצב להן, לשנות את סדר הפעולות, או לקרוא נתונים ולאחסנם בזיכרון. ישנם שני סוגים של מרחבי כתובות:

(1) זיכרון אמיתי
(2) זיכרון בפועל

בהגנה על זיכרון אמיתי, מחולק הזיכרון למחיצות בלעדיות שהגישה אליהן מבוקרת. כאשר תוכנית מתבצעת, הפקודה הנוכחית נמצאת באוגר הפקודה. היע"מ בוחנת את האוגר וקובעת את הכתובת בזיכרון שבה תתבצע הפקודה. לכתובת בזיכרון, שבה תתבצע הפקודה, צריכים להיות המאפיינים הבאים:

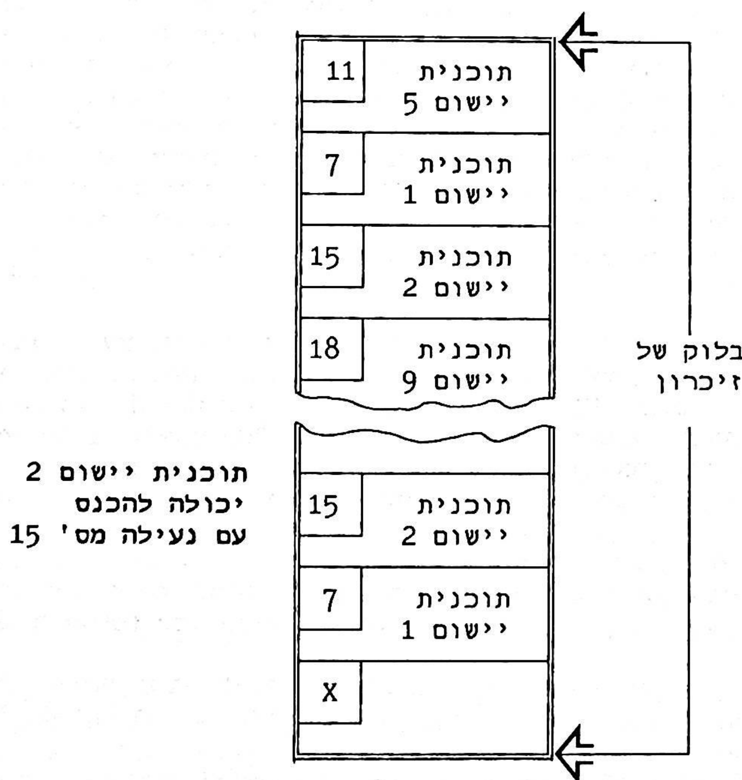
(1) מאפייני ההגנה צריכים להיות זהים לאלה שהוקצו לתוכנית שרצה.
(2) הכתובת צריכה להמצא בתוך השטח שצויין.

אם המנגנון להגנת החומרה מגלה טעות בכתובת או במאפייני ההגנה, היע"מ לא תשלים את ביצוע הפקודה. דבר זה יגרום לפסק (interupt) לא חוקי בחומרה וביצוע התוכנית יופסק.

אפשר להגן על הזיכרון בעזרת המנגנונים הבאים:

* אוגר גבול
* נעילות ומפתחות
* סיביות לבקרת כניסה

אוגרי גבול הם קבוצה של אוגרים ביע"מ המצביעים על שטח בזיכרון ומספקים אמצעים להקצאת מאפייני הגנה לאותו שטח ואמצעים להגדרת מעקב אחרי השטח המוגן. מערכות מחשב רבות משתמשות באופן כלשהו של אוגרי גבול. בדרך כלל מצביע אוגר אחד על תחילתו של השטח והשני - על גודלו. היע"מ משתמשת באוגרים אלה לחישוב הגבול העליון והגבול התחתון של השטח המוגן. הכתובת היחסית בפקודה חייבת להיות בתוך גבולות אלה, ולא - תחסם בפניה הגישה לזיכרון. מנגנון פשוט זה יעיל מאוד, אבל לכל זוג של אוגרי גבול נדרש אוגר נוסף, לאפיין הגנות נוספות, כמו זיכרון לקריאה בלבד.



תרשים 4.1 הגנת זיכרון באמצעות נעילות ומפתחות

נעילות זיכרון הם מספרי זיהוי המוקצים לשטחים של זיכרון אמיתי. בכל זמן נתון, אפשר להקצות מספר זיהוי מסוים לשטח אחד או יותר בזיכרון האמיתי, כדי שהתוכנית שרצה באותו זמן תוכל להשתמש בו (ראה גם תרשים 4.1). דבר זה סותר את עיקרון אוגרי הגבול, שלפיו התוכניות משתמשות בשטחי זיכרון רציפים.

כדי שתוכנית יישום תוכל להכנס לשטח, עליה לספק את המפתח. היתרונות של הגנה בעזרת מנעולים ומפתחות:

(1) תוכנית אחת יכולה להשתמש בשטחים שונים ומפוזרים.
(2) אפשר ליצור הירכיה של מפתחות. לדוגמה, מפתח מס' 1 יוכל לפתוח את כל הנעילות, ואף מפתח פרט למפתח מס' 1 לא יוכל לפתוח את נעילה מס' 1. מערכת ההפעלה יכולה להיות הבעלים של מפתח מס' 1 והיא נמצאת בזיכרון, בשטח המוגן בעזרת נעילה מס' 1.

מספר הנעילות האפשרי במערכת קשור תלוי ישירות במספר הסיביות המשמשות את מספרי הזיהוי. אם מספר הסיביות קטן, קטן גם מספר הנעילות שניתן להשתמש בהן. בנוסף, אם זיכרון אמיתי גדול משולב במספר קטן של נעילות, השטחים הנעולים יהיו גדולים והשטחים המפוזרים יהיו מעטים. דבר זה אינו מאפשר הקצאה גמישה של זיכרון והגנה על שטחים קטנים בזיכרון. אחת השיטות להתגבר על בעיות אלו היא שימוש בסיביות בקרת כניסה, שמהוות חלק מכל שטח בזיכרון. מבנה כזה מאפשר הגנה על שטחים קטנים ביותר מחד, ומאידך - נוצר, לכאורה, בזבוז של שטח אחסון בזיכרון.

בהגנה על זיכרון אמיתי קשה לאפשר לתוכניות יישום שונות דרישות אבטחה שונות, לגבי אותו שטח בזיכרון. לדוגמה, שתי תוכניות (המוגדרות כ"נתינים" בסעיף 3.3) נכנסות לנתונים משותפים ("אובייקט" משותף): התוכנית הראשונה תהיה כפופה לדרישות פחות מחמירות, כמו כתיבה וגם קריאה, ועל התוכנית השניה יוטלו מגבלות חמורות יותר, כמו קריאה בלבד.

כך גם במקרה של תוכנית המחזיקה במפתח כניסה לשני שטחים נעולים. בקרת הגישה נעשית על ידי הקצאת מאפייני הגנה נפרדים (ואף שונים) לכל שטח לדוגמה:

* קריאה בלבד לשטח הראשון.
* קריאה וכתיבה לשטח השני.

אפשר להתאים דרישות אלו לזיכרון בפועל, כדי לספק הגנה על שטחים גדולים של זיכרון בפועל, כמו סגמנטים, ועל שטחים קטנים יותר, כמו דפים וחלקים של דפים.

4.1.2 מצבי עיבוד מרובים (Multiple execution states)

רצוי שלתוכנות התשתית של המערכת, ובכלל זה מערכת ההפעלה, יהיו זכויות אכיפה (override) על תוכניות אחרות. תוכניות שצריכות זכויות כאלה:

* תוכניות גרעין קריטיות, כמו תוכניות ניטור ופיקוח ששולטות על ביצוע תוכניות אחרות.
* פקודות, כמו פקודות קלט/פלט, שהשימוש בהן כפוף להרשאות מסוימות.

תוכניות אלו אינן נמצאות בקביעות בשטח אחד, ולכן לא מספיק להגן עליהן ועל הביצוע שלהן רק בעזרת מנגנוני הגנה לזיכרון. יש להוסיף אמצעים שיבטיחו שתוכניות יישום לא יוכלו לבצע פקודות שיש צורך בהרשאה לביצוען. כדי להשיג זאת, משתמשת מערכת ההפעלה בטכניקות הבאות:

(1) מצב עבודה בינארי, או
(2) היררכיה של מצבי עבודה

טכניקות אלו משמשות את מערכת ההפעלה כדי לדעת אם היא מתבצעת במצב מועדף או במצב רגיל.

מצב עבודה בינארי הוא דרך פשוטה ליצירת סביבה שמאפשרת הקניית זכויות אכיפה. בסביבה זו ישנו מצב עבודה מועדף אחד ומצב עבודה שני לשאר השימושים. רק במצב מועדף, תוכל תוכנית לבצע פקודות מועדפות.

בטכניקה השניה, יכולות תוכניות להמצא בכמה מצבי עבודה, שההבדל ביניהם הוא בסוגי ההרשאות המוקנות לתוכנית, בכל מצב. לדוגמה:

* הרמה הגבוהה ביותר - לתוכנית פיקוח שאחראית על פסקי תוכנה וחומרה.
* הרמה השניה בחשיבותה - לתוכניות פיקוח שמטפלות באיתחול תוכניות, סימון וניהול העבודה.
* הרמה הבאה - למהדרים ולתוכניות עריכה.
* הרמה הנמוכה ביותר - לתוכניות יישום של המשתמש.

פרוייקט Multics הוא מנגנון המאפשר היררכיה של מצבי עבודה שיושם עם טבעות Multics במערכת Honeywell 6000 (אדלמן, 1976). ארכיטקטורה של מספר מצבי עבודה מאפשרת מצב של שיתוף משאבי מערכת במצב של חוסר אמון הדדי.

4.2 תוכנת המערכת

כל היישומים המסחריים מסתמכים מאד על תוכנות התשתית של המערכת. תוכנת מערכת, המסופקת בדרך כלל על ידי יצרן המחשב, כוללת מהדרים ותוכניות שירות. אך יש לזכור שבמונחים של אבטחה, המרכיב החשוב ביותר הוא מערכת ההפעלה. מערכת ההפעלה היא מערכת מקיפה ומורכבת הבנויה ממודולים של תוכניות, המאפשרות לתוכנה היישומית להשתמש במשאבים של מערכת המחשב. מערכת ההפעלה כוללת את המרכיבים הבאים:

* תוכנית ניהול שמתחילה ומסיימת תוכניות יישום ואף מקצה להן שטחים בזיכרון המרכזי.
* מערכת לבקרת קלט/פלט שמופעלת לפי פקודת תוכנית היישום וגורמת להעברת הנתונים מרשת התקשורת, או מיחידה היקפית, לתוך הזיכרון המרכזי - ולהיפך.

מערכת ההפעלה מטפלת בפעולות המחשב השונות. היא מפקחת על ביצועי החומרה כדי להבטיח ביצוע תקין וסיום של תוכניות. היא מטפלת במצבים של הפסקת פעולתה של תוכנית, דיווח והכנת המערכת לאיתחול של תוכניות אחרות. תוכנית הניהול יכולה להיות קשורה לבקר תקשורת, כדי אפשר למסופים מרוחקים או למחשבים אחרים להשתמש בתוכניות היישום ו/או במערכת לניהול בסיס הנתונים. במשך שנים רבות כיוון הפיתוח הוא להוציא משימות מידי המשתמשים ולספקן באמצעות מערכת ההפעלה. כתוצאה מכך, הופחתה הסכנה לפרצה באבטחה, מכיוון שהמשתמש פחות מעורב בפעולת המכונה. עם זאת, נוצרה סכנה גדולה יותר, כי קיימת אפשרות לטפל במשאבי המחשב בעזרת אמצעים של מערכת ההפעלה.

טבלה 4.2 גורמים המגדילים את הפגיעות של מערכת ההפעלה

(1)	תכנון לקוי, שגורם לפגעים רבים במערכת ההפעלה.
(2)	מערכת ההפעלה גדולה ומורכבת.
(3)	מערכת ההפעלה חדשה, וכתוצאה מכך - טרם נוסתה ונבדקה במידה מספקת.

מערכת ההפעלה יכולה לשלוט בכל משאבי המחשב ולכן חדירה אליה תאפשר גישה לשטחים של משתמשים. בטבלה 4.2 אפשר לראות גורמים המשפיעים על הפגיעות של מערכת ההפעלה. אולם, כדי שמישהו יוכל לנצל את חולשותיה עליו להיות בעל ידע ומניעים ובעל אפשרות גישה. לצערנו, בכל מתקן מחשב נמצאים אנשים המחזיקים בידע על התוכנה ועל שאר המאפיינים שצוינו. אנשים אלה יכולים

לעקוף את הבקרות של מערכת ההפעלה (שרף, 1980). לכן מעסיקה אבטחת מערכת ההפעלה גורמים רבים מזה עשור ויותר.

מערכת הפעלה שמכילה טעויות תכנון, או שהפעילות שלה פגיעה, אינה יכולה להוות בסיס חזק ואמין לבניית מערכת מידע. אולם מערכת הפעלה שמתוכננת היטב היא חלק חיוני ופעיל בהגנה על מערכת המידע. בסעיף הבא נדון בעקרונות של מערכת ההפעלה, כדי לראות כיצד היא יכולה לתרום לאבטחה של מערכת המידע, בביצוע הפעולות הבאות:

* בקרה על משתמשים ותוכניות: רק משתמשים מורשים ותוכניות מורשות יוכלו להכנס למשאבי מחשב ספציפיים.
* מניעת ניסיונות, מכוונים ולא מכוונים, של משתמשים ושל תוכניות לפנות לשטחים שאין להם אישור לפנות אליהם.

4.3 פונקציות האבטחה של מערכת ההפעלה

אפשר לסווג את פונקציות האבטחה של מערכת ההפעלה בשתי קבוצות:

(1) פונקציות שאינן קשורות באופן ישיר לאבטחה.
(2) פונקציות ייעודיות לאבטחה.

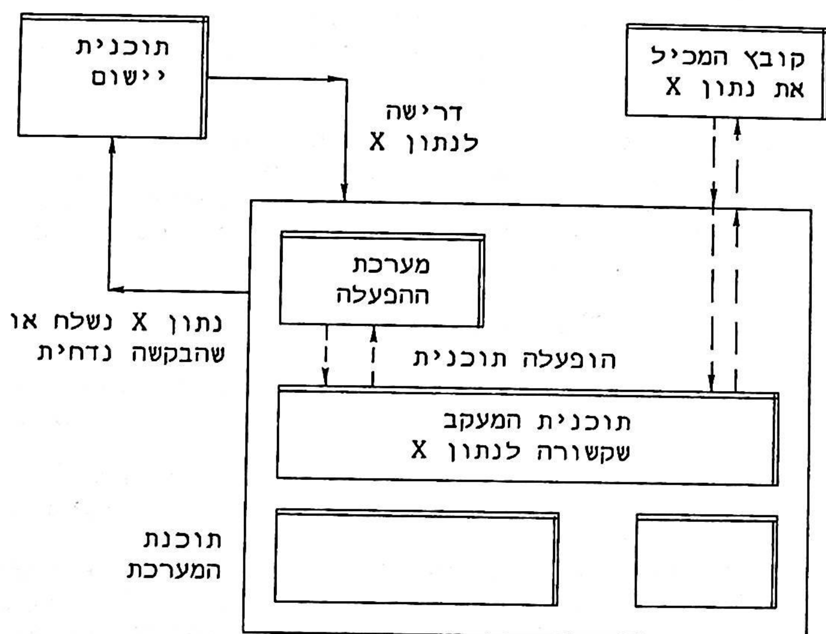
הפונקציות שאינן קשורות באופן ישיר לאבטחה הן אלו שמנהלות ומבקרות את משאבי המערכת ותוכניות היישום. הן כוללות את תוכנית הניהול ואת השגרות שאחראיות על תזמון, הקצאת משאבים, הקצאת זיכרון, קלט/פלט ותמיכה בתקשורת. הייעוד של פונקציות אלו הוא ניהול ובקרה של משאבי החומרה של המערכת, במטרה ליצור סביבה מתאימה להרצה של תוכניות יישום. הפונקציות שיש להן קשר ישיר לאבטחה כוללות:

(1) מעקב וזיהוי,
(2) בקרת גישה (כניסה למערכת),
(3) בידוד (isolation).

4.3.1 ניהול של משאבי חומרה - מעקב

על מערכת ההפעלה לזהות באופן חד משמעי את המשתמש ואת משאבי המערכת. אפשר לזהות משאבים בעזרת השיטות שתוארו בסעיף 4.1. על מערכת ההפעלה לבצע את הפעולות הבאות, כתגובה לפניית משתמש:
* לקשר את המשתמש למשאבים שהוא מורשה להכנס אליהם.

* להקצות למשאבים מאפייני הגנה מתאימים, כמו קריאה בלבד או קריאה וכתיבה, בזמן ההרשאה למשתמש.
* לקבוע במהלך ביצוע תוכנית, כאשר קיימת בקשה למשאבים, אם לאשר את הבקשה או לדחות אותה. פעולה זו מתבצעת על ידי בדיקה של זהות המשתמש, של המשאבים המבוקשים ושל מאפייני ההגנה שהוקצו למשאבים.



תרשים 4.2 המעקב המתבצע על ידי מערכת ההפעלה

בנוסף לנוהלי הזיהוי, מבצעת מערכת ההפעלה נוהלים המאפשרים רישום וניטור של איומים.

פעילות האבטחה של מערכת ההפעלה לא מסתיימת לאחר שהיא מאשרת בקשה של תוכנית שרצה; היא חייבת עדיין לפקח על הפעולות המבוקשות עד שיסתיימו. לדוגמה, אם תוכנית קיבלה אישור גישה לבסיס נתונים סטטיסטי, אפשר לתת לה להכנס לנתונים בעזרת שגרת העיבוד שלה או בעזרת שגרה של המערכת. האחרונה מאפשר למערכת ההפעלה לבקר ולנטר את אופן השימוש במשאבי המערכת. במצבים כמו גישה לבסיס נתונים, זה עשוי להיות קריטי. כמתואר בתרשים 4.2, ניתן להעניק לתוכנית המעקב או הניטור סמכויות רחבות יותר מאשר פיקוח בלבד, כדי ליעל את פעולתה. במקרה של בסיס נתונים, הסמכויות הנוספות יכולות לכלול את האפשרות

לנטר:

* מאפיינים חופפים של נתונים בשאילתות המבוצעות זו אחר זו.
* מספר השאילתות שהמשתמש יכול לבצע.
* ערכי המינימום והמקסימום של הנתונים שנאספו.

החשיבות של נקודות אלו, הקשורות לסכנות שבהיקש לוגי מתוך בסיס נתונים, מוסברת בפרק 3. כדי להשלים את ניטור האיומים, חייבת מערכת ההפעלה לבצע רישום של כל מושב הידברותי (Interactive processing session) ושל כל מושב באצווה (Batch processing session). שיטת הרישום לשם מעקב ופיקוח מוסברת שוב בפרק 6. המידע שנרשם חשוב מאוד ויש להגן עליו בצורה מיוחדת.

4.3.2 בקרת כניסה

תוכנית היישום שרצה במערכת צריכה לבצע את הפעולות הבאות:

(1) לפנות לזיכרון אמיתי או לזיכרון בפועל. דבר זה מטופל על ידי החומרה, כפי שכבר הוסבר.
(2) לקרוא לתוכניות ולקבצים. החומרה אינה יכולה לטפל בפעולות אלו לבדה ולכן מערכת ההפעלה מטפלת בהן. מערכת ההפעלה מנהלת קריאות לתוכניות וקבצים בעזרת טבלת הרשאות, שהוסברה בסעיף 3.3.3.

4.3.3 בידוד

בגלל ריבוי הדרישות, מערכת ההפעלה היא תוכנה מורכבת מאוד וכידוע, שילוב של ריבוי ומורכבות עלול לגרום לדליפת נתונים ולנפילת המערכת. לכן, הגישה בתכנון מערכת הפעלה היא להפריד בין החומרה לבין התוכנה, כדי שכל אחת מהן תוכל להוציא לפועל את משימותיו בנפרד. המטרה היא לבודד את הפרצה באבטחה לתא שבו התרחשה, כדי ששאר חלקי המערכת לא ייפגעו. ההנחה הבסיסית בגישה זו היא שהזמן שנדרש לבניית כמה מערכות קטנות, או מערכת מונוליתית גדולה, זהה. לכן עדיף לבנות כמה מערכות קטנות, מכיוון שהתוצאה הסופית הינה מערכת בטוחה יותר. הגישות שעוזרות ביישום השיטה:

(1) גישת המרחבים הרבים (multiple space method).
(2) גישת המכונה בפועל (virtual machine).
(3) גישת הגרעין (the kernel concept).

בגישת המרחבים הרבים, כל קבוצה של תוכניות יישום רצה במחיצה נפרדת של הזיכרון הראשי, אך כל תוכניות היישום מבוקרות על ידי אותה מערכת הפעלה. אם מודול של תוכנית נדרש במחיצות נפרדות, נוצר עותק משוכפל של אותו מודול בכל מחיצה. מערכת ההפעלה אינה משוכפלת והניטור של משאבי המערכת והנתונים המשותפים נעשה על ידי מערכת הפעלה מרכזית. אם מיישמים גישה זו ביחד עם מרחבים רבים בפועל, תופיע מערכת ההפעלה בכל מרחב בפועל ללא שכפול. מערכת ההפעלה המרכזית היא המערכת היחידה שבה משתמש המחשב לרישום, לבקרת גישה ולבקרה כללית. אופן עבודה זה אינו עוזר לפשט את מערכת ההפעלה. אם מתבצעת חדירה למערכת ההפעלה המרכזית ייחשפו כל המחיצות להתקפה (מקפי, 1974).

בגישת המכונה בפועל, יש לכל מחיצה מערכת הפעלה נפרדת. במערכת מחשב שפועלת לפי גישה זו, יכולות לפעול כמה מערכות הפעלה. בקר המכונה בפועל שולט בתהליך. לטכניקת הבידוד, לפי גישה זו, כמה יתרונות:

* קשה יותר לחדור, כי יחסית, קל להגן על תוכנית הפיקוח.
* אפשר להשתמש בכמה מערכות הפעלה, בהתאם לדרישות האבטחה.
* אם תתבצע חדירה למערכת הפעלה אחת, תפגע רק המחיצה שבה היא נמצאת וכל יתר המחיצות יישארו ללא פגע.

אפשר להגיע לבידוד בדרכים נוספות. לדוגמה, קבוצת יישומים מסוימת תופעל רק כמה שעות ביום. אפשר גם להפריד פונקציות, כמו בין אלו של שיתוף זמן לבין אילו של עיבוד באצווה; אופני בידוד אלו נקראים, בהתאמה, בידוד התלוי בזמן ובידוד התלוי במרחב.

4.4 אימות תוכנה, גישת הגרעין ובדיקת חדירות

מערכת הפעלה יכולה להיראות מושלמת על הנייר, אך לא נהיה בטוחים שהיישום שלה תואם את התכנון הראשוני. טכניקות אימות משמשות לבדיקה של תקינות התוכנה (לוקש וסייבר, 1984). כללית, יישומי תוכנה הם מכלול של הצהרות על דרישות ונכסים (במקרה זה - נתונים), יותר מאשר שגרות המשמשות לבניית תוכנה. לכן, טכניקות האימות מתרכזות בהשוואה בין דרישות התכנון לבין יישומן בפועל. בדרך כלל, אימות של כל מערכת ההפעלה איננו אפשרי מבחינה כלכלית או טכנית, בגלל הגודל והמורכבות של המערכת. אחת האלטרנטיבות היא לבודד כמה פונקציות שחיוניות לפעולה הבטוחה של מערכת ההפעלה וליצור מהן מערכת הפעלה פשוטה, אך מושלמת, שתקרא "גרעין האבטחה" (שרף, 1980). התכונות של הגרעין צריכות להיות:

(1) שלם. כל הכניסות ייבדקו על ידי הגרעין.
(2) מבודד. כל תוכנה אחרת לא תוכל לשנות את הקוד שלו.
(3) תקין. יבצע את כל הפונקציות שנדרשות ממנו, אך לא יותר.

הרעיון המרכזי הוא לבדוק את כל החלקים החיוניים של מערכת ההפעלה, הגרעין. הבעיה המרכזית בגישה זו היא להגדיר את הפונקציות הבסיסיות שיוצרות את הגרעין.

כדי לקבוע שתוכנה כלשהי בטוחה, יש להוכיח זאת בצורה מתימטית. לצערנו, אימות תוכנה קשה מאוד, וגם אם שיטות האימות קובעות שהמערכת תקינה, אין זה מבטיח שמערכת ההפעלה בטוחה. אפשר להשתמש בבדיקת חדירות, כדי לנסות לזהות את נקודות התורפה (אטנסיו, 1976). בדיקות אלו ישיגו בטחון רב יותר במאפייני האבטחה של מערכת ההפעלה. הסכנה בשיטה זו היא שתהיה תמיד בדיקת חדירות אחרת ועל כן שתוחמצ, ויש להתייחס לבטחון זה בהסתייגות.

מן הראוי להוסיף שהדיון שהתייחס למערכת ההפעלה טובה גם למערכת תוכנה, או יישום. יש ליצור מערכת מובנית, שבה יהיה גרעין שולט ומפקח ומודולים שיבצעו פונקציות מוגדרות ופשוטות. כך אפשר לבודד חלקים של מערכת התוכנה, הן לצורך ניהול ואחזקה והן לצורך אבטחה.

4.5 תקשורת

אפשר לבצע תקשורת נתונים בדרכים רבות. לדוגמה, על ידי הדואר ו/או שליח, או באמצעות מערכת הטלפונים. בסעיף זה נתעלם מתקשורת נתונים באמצעות תעבורה פיסית ונתרכז בטלקומוניקציה, או תקשורת באמצעות מחשוב. כשנולדה תקשורת הנתונים, שודרו כמויות נתונים קטנות יחסית, שכללו כמות קטנה מאוד של מידע סודי. במהלך הזמן הפכו מערכות המחשבים והתקשורת לחלק בלתי נפרד מהמגזר העסקי, ושידור של מידע סודי הפך לנפוץ יותר. לצערנו, צפויות שיטות השידור לאיומים הבאים:

* יירוט נתונים
* שינוי נתונים
* ציתות

מידע משודר טיפוסי מתייחס לנתונים עסקיים, לחשבונות בנקים, לפרטים אישיים על אנשים לרשומות רפואיות ועוד. במלים אחרות, נתונים אלה ואחרים רגישים ויש להגן עליהם בכל הרמות בין המשדר למקבל. לכן, דרושה מערכת תקשורת בטוחה שבה הודעה שתשודר תחזיק בתכונות הבאות:

* עליה להגיע למקבל שאליו היא יועדה בלבד.
* על התוכן שיגיע למקבל המיועד להיות זהה לזה ששודר במקור.
* אדם לא מורשה לא יוכל לעכב אותה, או לפענח אותה, במהלך השידור.

טבלה 4.3 אבטחת התקשורת

סוג האיום	איום	פגיעה	אמצעי נגד
לא מכוון	שגיאות בשידור, רעש, תקלות בקו או במודם הודעה נשלחה ליעד אחר מזה שנקבע לה	שלמות נתונים וזמינות של שירותים סודיות, הפרעה לשירותים	נוהלים לגילוי ולתיקון שגיאות ניתוח תקלות נוהלי התחלת עבודה ממסוף מרוחק
מכוון	התקפה פיסית	זמינות של שירותים	ציוד כפול, כמו קו חליפי בקרות כניסה פיסיות ועוד.
מכוון	האזנה אקטיבית (לדוגמה, שינוי נתונים וכניסה למידע חסוי) האזנה פסיבית (לדוגמה, ניטור התקשורת על ידי לא מורשים)	סודיות שלימות הנתונים סודיות	הצפנה, ניטור קווים ובקרות כניסה פיסיות

למשל, בסביבת התקשורת מבוקרים אמצעים רבים על ידי צד שלישי, כמו חברת בזק, וולכן המשתמש אינו יכול לקבוע אם לשירותים שניתנים יש מאפייני אבטחה כנדרש. למרבה המזל, קיימים אמצעי אבטחה, כמו הצפנה, שמאפשרים הגנה על מידע רגיש. בנוסף לכך, אם ייעשה שימוש ברשת הטלפון הציבורית, תהיה סבירות נמוכה יותר לחדירה במקומות המרוחקים מצמתי החיבור של המשדר והקולט בגלל המורכבות ברשת. במקרים כאלה סביר להניח שהעבריין הפוטנציאלי יחדור לרשת במקומות הקרובים למסוף, כי רק בנקודות הקצה של הרשת אפשר לזהות וליירט נתונים.

4.5.1 פגיעויות, איומים ובקרות

הפגיעות גדלה במצבים שבהם ארגון תלוי מאוד בתקשורת נתונים. הבעייה מסתבכת כאשר קיים שילוב של הזנת עבודות מרחוק, שיתוף זמן ותקשורת בין מחשבים. הבעיה מורכבת גם במקומות שבהם קיימת רשת מחשבים מבוזרת שמשתמשת בחומרה של ספקים שונים ופרוטוקולים שונים לתקשורת.

כמצויין בטבלה 4.3 ובתרשים 4.3, האיומים צפויים מכיוונים שונים. כאשר משתמש מורשה מטפל במידע שמאושר לשימושו דרך מסוף מורשה, קיימת סכנה שהנתונים יאבדו, יועתקו או ישונו במהלך השידור. אם רשת התקשורת מפוזרת על פני איזור גיאוגרפי גדול, היא חשופה יותר להפרעות חשמליות, להפרעות מזג האוויר ולפעילות אנושית מזיקה. ניתן לזהות שלושה איומים עיקריים לבטחון התקשורת:

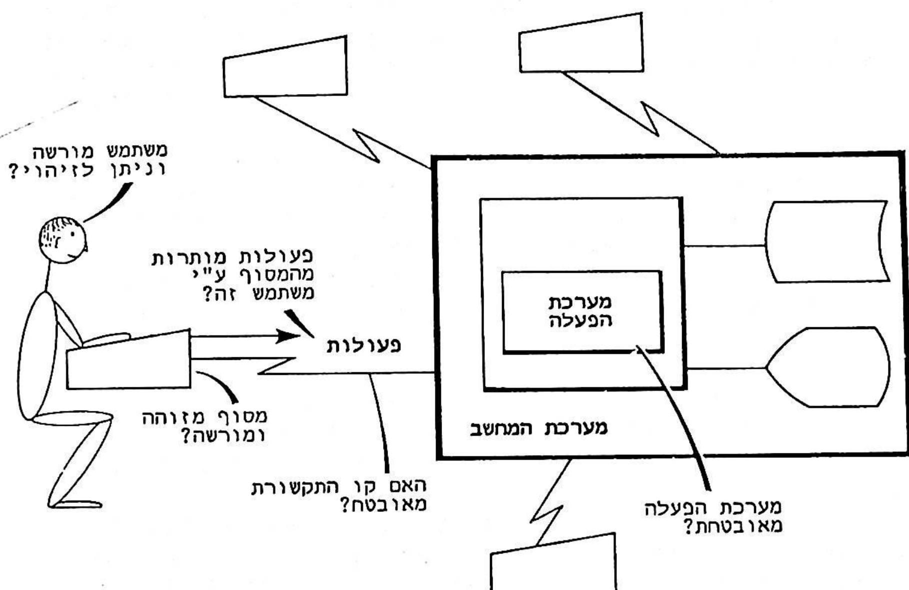
(1) רעש, שממסך והורס את משמעות הנתונים המשודרים.
(2) יירוט ההודעות, שמאפשר למצותת להשיג מידע חסוי.
(3) ניתוק, שמשמעותו הפסקת השירות ואובדן של הודעות.

בקרות אבטחה שניתן ליישם בהתאמה בשלושת המצבים שהוזכרו: קודים לגילוי שגיאות, כמו בדיקת זוגיות; הצפנה וציוד אלטרנטיבי למקרה של תקלות. פרצות טכניות ברשת התקשורת דומות לאלו שבמערכת ההפעלה, בכך שרק אדם מיומן מאוד יוכל לנצלן. כדי לעמוד בפני פורץ ולשפר את מצב האבטחה באופן משמעותי, אפשר להתקין בקרות פיסיות ונוהליות בכל נקודת חיבור לרשת. מתכננים של מערכות מידע מודעים בדרך כלל ליתרונות של שיטות טכניות, כמו הצפנה, אך אין להם עוסקים בבקרות נוהליות, פיסיות ומנהליות. מכל מקום בתקשורת נתונים ישנו תמיד צורך באמצעים טכניים לאבטחה וזאת כדי להשיג העברת הודעות תקינה ואמינה. השיטות כוללות פרוטוקולים לתקשורת, שיטות שידור ותוכנה לתקשורת נתונים הנתמכים על ידי:

(1) קודים לגילוי שגיאות כמו בדיקת זוגיות ובדיקת פולינום,
(2) אפשרות לשידור חוזר, במהירות נמוכה, אם העברת ההודעה לא הסתיימה בצורה מספקת,
(3) ערוץ שידור אלטרנטיבי,
(4) ניהול התקשורת, הפיקוח עליה והתחזוקה יהיו באחריות צוות אחד.הדבר חשוב במיוחד אם ספקי החומרה הם רבים.
(5) גיבוי או ציוד אלטרנטיבי שישמש בעת הצורך כתחליף לציוד חיוני.

שיטות אלו משולבות כדי ליצור סביבת תקשורת אחידה ויעילה,

שבה מספר השגיאות יהיה מינימלי והשגיאות שכן יקרו - יתגלו ויתוקנו.



תרשים 4.3 האבטחה של מערכת המחשב

4.6 מסופים, עיבוד נתונים מבוזר והשפעת האבטחה על מערכות מקוונות

השירות שסיפקו מערכות מחשב מרכזיות בשנות השישים היה עיבוד קונבנציונלי באצווה. הנתונים שנשמרו במחשב היו קלים לתחזוקה, באופן יחסי, ולמערכת יכלו לגשת רק אלה שהצליחו להכנס לחדר המחשב. לכן, מטרת האבטחה היתה להגביל את הכניסה למשתמשים מורשים בלבד, למרות שלא היה בכך כדי למנוע ממשתמשים מורשים לנצל זכות זו לרעה. בקרת כניסה התבססה על המרכיבים הבאים:

* צוות מרכזי לבקרת עבודות, שקיבל עבודות מהמשתמשים וכך ניתן היה לזהות אותם באופן ישיר.
* כרטיס עבודה החתום על ידי משתמש מורשה.
* מפעיל מחשב, שהיה אחראי לקבלת העבודות, להכנסתן למערכת, להרצה ולביצוע של כל עבודה.

טבלה 4.4 גורמים המגדילים את הפגיעות של מערכות מקוונות

(1) בעיות בזיהוי ובהרשאה של משתמשים מורשים.
(2) בעיות באכיפת נוהלי אבטחה זהים, באתרים שמפוזרים במרחב גדול.
(3) המשתמש מחזיק באפשרות של תכנות מאתרים מרוחקים.
(4) ביצוע פעולות מתוחכמות ממרחק. לדוגמה, שיתוף-זמן, הכנסת עבודות מרחוק (RJE) ועיבוד תנועות.
(5) נתיבי ביקורת חלשים.
(6) קווי התקשורת פתוחים לחדירות ולהאזנות.

שיפורים בטכנולוגיית המחשב ודרישות לזמני תגובה מהירים יותר ולשירותים מבוזרים הביאו לכך שמערכות יישומיות עברו מעיבוד באצווה לעיבוד מקוון. במערכות מחשב מקוונות, מספקים המסופים כניסה לאובייקטים הבאים:

* למערכת עיבוד נתונים מרכזית.
* למערכת עיבוד נתונים מבוזרת שכוללת אמצעים לביזור יכולת העיבוד, מסופים להזנה של עבודות באצווה ממרחק, מסופים להכנסה ישירה של נתונים ורשת של מחשבים ובסיסי נתונים.

ההצלחה של מערכות מקוונות נובעת משתי סיבות:

(1) הן מאפשרות הידברות, וכך מתבצע שימוש ישיר במשאבי המחשב.
(2) הן מתגברות על בעיות של מרחק.

לצערנו, במערכת מקוונות אי אפשר להשתמש בבקרת כניסה מרכזית, כמו במערכות המתבססות על עיבוד באצווה. מערכת מקוונת מגדילה את פריון העבודה ואת היעילות של שירותי העיבוד, אך יוצרת בעיות אבטחה חדשות. מבלי להתייחס לתצורה של עיבוד הנתונים המבוזר ומבלי לדון בשאלה אם נעשה שימוש בעיבוד נתונים מבוזר או מרכזי, ברור לכל שהשימוש במסופים סיבך את בעיות האבטחה ושינה את ההיקף ואת האופי של הפגיעויות והאיומים.

4.6.1 מסופים - פגיעויות ואיומים במערכות מקוונות

תמצית הבעיה בהגנה על מערכת מקוונת היא מחסור בבקרות על קהיליית המשתמשים, או פגיעות הבקרות הקיימות. בטבלה 4.4 אפשר לראות גורמים המגדילים את הפגיעות. במצבים רבים משתלבים גורמים אלה יחדיו ויוצרים איום גדול על האבטחה. איומים טיפוסיים, כמתואר בטבלה 4.5, גורמים לפגיעות באבטחה:

* הכנסה של תנועות שקריות, שיכולות למשל, לספק לאדם תשלומים שאינם מגיעים לו.
* השחתה של קבצי נתונים.
* שימוש בשירותי מחשב ללא תשלום על ידי אדם המתחזה למשתמש מורשה.
* שימוש בשירותי המחשוב ללא הרשאה לצורכי שימוש עסקי פרטי, לשם שעשוע וכד'.

אלו הן בעיות קשות בגלל אופיה המורכב של מערכת מקוונת, שאבטחתה תלויה באבטחת החומרה, מערכת ההפעלה והתקשורת ובנוהלי זיהוי והרשאה (ראה גם תרשים 4.3).

4.6.2 בקרות

אפשר להשתמש בטכניקות ובנוהלים שונים כדי לצמצם את האיומים לאבטחה של מסופים מרוחקים ומערכות מקוונות. בטבלה 4.5 תמצא פירוט של אמצעי הנגד שנדון בהם בתת-סעיף זה. הם כוללים:

* אבטחה פיסית
* בקרת כניסה
* הגנה מפני תקלות במסוף
* בקרות נוהליות
* ניטור איומים
* טכניקות בידוד

טבלה 4.5 אבטחת מסוף

סוג האיום	איום	אובדן	אמצעי נגד
לא מכוון	תקלה במסוף	שלימות נתונים, זמינות של שירותים	תחזוקה מונעת ושוטפת וגיבוי (מחשב נוסף)
	טעויות אנוש והשמטות	שלימות נתונים, זמינות של שירותים	הדרכה ותרגול
	אסון טבע	זמינות של שירותים	אמצעי נגד פיסיים (ראה פרק 2)
מכוון	התקפה פיסית הגורמת לנזק או לגניבה	זמינות של שירותים	בקרות כניסה פיזיות וציוד חליפי
	שימוש ללא הרשאה במסוף במסוף, שגורם לגניבת זמן מחשב וקבצים	סודיות, שלימות הנתונים	בקרות כניסה פיסיות, סיסמאות, נעילת מסופים ונוהלי זיהוי והרשאה
	הצצה בנתונים בנתונים על המסוף שעלולה לגרום לשימוש לא מורשה במידע סודי	סודיות, זמינות של שירותים	בקרות כניסה פיסיות, דיאלוג אדם-מכונה ומיקום של מסופים

בסביבה מבוזרת, אחת המשימות החשובות היא אבטחת כל אתר מרוחק. לשם כך, באתרים המרוחקים יש ליישם, עד כמה שאפשר, את הסטנדרטים של האבטחה הפיסית שמיושמים במתקן המחשב המרכזי. אין זה פשוט, כי החומרה שמפוזרת באתרים השונים - כמו מחשבים קטנים ואישיים, מסופים להכנסת עבודות מרחוק ומסופים הידברותיים וחכמים - ממוקמת באיזורים הפתוחים לכל, עם הגנה פיסית מינימלית. מומחים לאבטחה מעדיפים שציוד שממוקם באתרים

מרוחקים ינעל מאחורי דלתות, יבוקר על ידי מפתחות, על ידי קוראי כרטיסים, או על ידי סיסמה. למשתמש יש יתרונות משלו בסביבת משרד פתוחה ולכן היא תשאר כזו. מדיניות ההנהלה תשמש בסיס חזק, שהוא חיוני לאבטחה. על המדיניות לכלול את הפרטים הבאים, לגבי כל אתר:

(1) למנות אחראי לאבטחה באתר.
(2) לציין את זהות אנשים המורשים להשתמש בציוד.
(3) לקבוע נוהלי כניסה מקיפים והרשאות של משתמשים.
(4) קביעת העונשים שיוטלו על המפירים את המדיניות שנקבעה.

את היקף הבעיה של אבטחה פיסית אפשר להקטין אם הציוד ימוקם בחדרים נפרדים, שאפשר לנעול אותם, ולא בשטח המשרדי הפתוח. יש גם לנתק את הציוד כאשר אין הוא נמצא בשימוש. אפשר לחדור למערכת באמצעות ציוד עקיבה מתוחכם, שקולט קרינה אלקטרו-מגנטית מהמסוף. בהווה אין זה חשוב עדיין, אך בעתיד, כאשר שיטות חדירה פשוטות יכשלו, תהפוך העקיבה האלקטרו-מגנטית לנחוצה יותר. בנסיבות אלו יש חשיבות גדולה לנטרול איום זה על ידי מיקום חדר המסוף במרכז הבניין, למשל. גם היום יש לכך חשיבות במתקנים סודיים, כמו אלה של הצבא.

לאחר שתבוקר הכניסה לחדר המסוף, אפשר יהיה לטפל בדרישה הבאה - מניעת שימוש במסוף עצמו, או בשירותי המחשוב האפשריים, באמצעות המסוף. אפשר להשתמש במסופים מאובטחים שניתנים לזיהוי ו/או שיש להם קוראי כרטיסים מובנים המאפשרים את זיהוי המשתמש. כרטיס הזיהוי של המשתמש הפוטנציאלי נקרא במסוף והמידע שהוא מכיל מועבר למחשב לאימות. המסוף יפסיק לפעול אם מוציאים ממנו את הכרטיס. בנוסף לכך, על המשתמש להכיר את נוהל השימוש בכרטיס שבידו. בפרק 3 קיים דיון על שיטות לזיהוי ואימות, כמו סיסמאות, למשל. אולם, אימות והרשאה של משתמשים חסרי תועלת ללא בקרות פיסיות ומנהליות מקיפות (ליין ורייט, 1979).

קשה ליישם בקרות מנהליות. המטרה היא לאכוף בצורה עקבית את נוהלי האבטחה, ולשם כך דרושה תוכנית הדרכה מתמשכת באבטחה (ראה פרק 5). על כל משתמש לעבור קורס הכוונה לאבטחה, שבו תוסבר לו חשיבות תוכנית האבטחה, תפקידו ואחריותו של כל משתמש בהשגת היעדים. הקורס מבוסס על מדיניות האבטחה של הארגון ומשלים אותה. המשתמש ילמד את הסטנדרטים של האבטחה בארגון, שחייבים להיות שלמים, עקביים וניתנים לאכיפה ולביקורת. נושאי ההדרכה הרלוונטיים למשתמשים במסופים:

* נוהלי אבטחה המתייחסים לטיפול, אחסון והשמדה של מידע וחומר סודי אחר.
* הגנה על סיסמאות.
* השוואת נתונים המסופקים על ידי המחשב בתחילת כל מושב (session) במסוף עם הנתונים שטופלו במושב האחרון.
* ניתוק המסוף בסיום מושב עיבוד, כדי להסיר את הסכנה של מסוף הנשאר מקוון ללא משתמש לידו.

יש ליצור ולתחזק קבצי רישום כרונולוגיים (log files), כדי לאפשר בקרה על הפעולות המבוצעות על ידי המשתמשים, התוכניות והמערכת. חלק מהרשומות הוזנו במכוון, כמו אלה שמתייחסות לנפילה של המסוף, לתחזוקה ולפעולה לא תקינה. שאר הרשומות מופקות על ידי המחשב, כמו אלו הקשורות לניטור איומים.

תחזוקה מונעת ומסופי גיבוי הם אמצעים נגד נפילת מסוף ופעולה לא תקינה בו. ציוד חירום נוסף הכרחי במסופים מסוימים, אך ההוצאות יהיו גבוהות מדי אם ידרש גיבוי לכל מסוף מרוחק. יש להתקין מסוף גיבוי רק במקרים חיוניים. לכן, יש לשפוט כל מקרה לגופו וההחלטה צריכה להיות מבוססת על פי החשיבות של העיבוד באתר.

אפשר להשתמש ביכולתה של מערכת ההפעלה להפיק רישומי ביקורת (ראה פרק 6). ניטור איומים (ראה סעיף 4.3.1) הוא פונקציית הגנה נוספת של מערכת ההפעלה, שבעזרתה רושמת המערכת אירועים. אם התנהגות המשתמש מהווה איום על המערכת, היא מנתקת אותו. כדאי אולי, לדאוג שמשתמשים יהיו מודעים להפעלת ניטור איומים, כי המצאותו תוכל לשמש גם כאמצעי הרתעה. ניטור איומים יוכל לבדוק דפוסי התנהגות חשודים. דוגמה לכך, המתוארת בתרשים 3.1, היא הספירה של המערכת את מספר הניסיונות הכושלים להכנס. אם מספר זה עולה על המותר, זו התרעה על כך שמישהו מנסה לנחש את הסיסמה.

השיטות שתוארו לעיל אינן מיועדות לשימוש בכל מתקן, בכל מקום ובכל זמן. באחריותו של מתכנן המערכות המקצועי להתקין אמצעי נגד שיתאימו לצרכים המיוחדים ולכל מצב. מצבים מסוימים דורשים הגנה קטנה מאוד ולעומתם, מצבים אחרים דורשים שיקולים מיוחדים, או הגנה מיוחדת. לדוגמה, סוג של בידוד (ראה סעיף 4.3.3) יהיה מתאים כאשר מסופים מסוימים משמשים רק לסוגים מוגדרים של תנועות, במשך פרקי זמן מוגבלים וכאשר מסופים, או ציוד אחר, משמשים רק ליישומים מסוימים, או עבודה בקבוצה סגורה של משתמשים שהתקשורת מותרת להם וביניהם בלבד.

4.7 סיכום

הבעיות בתוכנת המערכת קשורות לבדיקת תקינות ולתכנון לא מושלם. בעיות אלו מחמירות יותר במערכת ההפעלה גדולה ומורכבת. מערכת הפעלה לאתר אחד ולמחשב אחד הפועלת באצווה בלבד, הינה קטנה הרבה יותר ופחות מורכבת מאשר זו המשמשת מערכת גדולה המריצה מספר רב של יישומים במקביל ועם תקשורת לאתרים רבים (השווה, לדוגמה את מערכת ההפעלה במחשב האישי, עם זו הפועלת במתקן המחשבים של משרד האוצר ורשת מס ההכנסה). הגודל והמורכבות של מערכת הפעלה קשורים באופן ישיר לסביבה התפעולית שלה. במצבים מסוימים הופכת מערכת ההפעלה למורכבת יותר, וככל שנעשים מאמצים ליצור מישק משתמש ברמה גבוהה יותר (כדי לאפשר גמישות ונוחות בשימוש), כך גדלה הפגיעות של המערכת ומתעורר הצורך באמצעי אבטחה מתוחכמים יותר.

בדומה, מורכבות התקשורת, שנובעת ממנגנוני הקישור השונים, ציוד מיתוג ואמצעים לניהול התקשורת, מגדילה את החשיפה של המערכת לאיומים. לדוגמה, התקשורת צפויה לעקיבה אלקטרו-מגנטית, הפרעות והאזנות. תוקף מומחה והחלטי יוכל להשתמש בציוד אלקטרוני מיוחד כדי לשדר אותות שישבשו את ההודעות וכדי לגלות אותות המשודרים ממסופים, כמו קרינה אלקטרו-מגנטית או כרעש. בנסיבות כאלה יש צורך בהגנה מיוחדת, שמעסיקה מאוד את האחראים למערכות מידע הקשורות לבטחון לאומי, אך חיונית פחות במערכות מידע המשמשות את המגזר העסקי. בקשר להאזנה, קשה למנוע מפורץ החלטי, אם ניתנה לו האפשרות להכנס למתקן, למצוא מקום שבו יוכל לצותת לקו. חשוב, לכן, להשתמש באמצעי אבטחה פיסיים, בדומה לאלה שנסקרו בפרק 2 כדי למנוע כניסה, וכך להקטין את האפשרות לציתות. לגבי מידע רגיש, יש להשתמש תמיד בהצפנה.

עיבוד נתונים מבוזר והשימוש במסופים מציעים מערכות ידידותיות למשתמש ויעילות גבוהה יותר של שירותי המחשוב, אבל אין הם מציעים אבטחה טובה יותר, כי הם עוקפים בקרות פיסיות. מערכות המשתמשות במסופים ובעיבוד נתונים מבוזר עשויות להיות בטוחות למדי. להוכחה - בנקים בכל רחבי העולם התקינו מסופים אוטומטים לחלוקת כסף (כספומטים) במקומות ציבוריים. מערכות מקוונות משנות את ההיקף והאופי של האיומים על המערכת. לדוגמה, בשירותי מחשוב הפועלים באמצעות קווי חיוג, יכול לקרות מצב שבו משתמש אחד נכנס למערכת ומנותק בטעות, ומשתמש שני, שהתקשר, "עלה על הקו" וחובר למושב של המשתמש הראשון, מבלי שעבר דרך תהליך האימות (AFIPS, 1979).

כניסה למערכת יכולה להיות "על חשבון" משתמש אחר (piggy-backing) "שלא סיים" (log off) את המושב שלו בצורה תקינה.

זו יכולה להיות פעולה מכוונת, בשיתוף פעולה בין אנשים, אך ברוב המקרים הדבר נגרם מצירוף מקרים. חשוב שרשתות יוכלו לגלות כניסה ויציאה של משתמשים, שאם לא כן, תתרחש חדירה ללא בקרה דרך הכניסות הרגילות (ports). על המתכנן להעריך את הסיכונים הקיימים במערכות מקוונות, כדי שיוכל לבחור בבקרות מתאימות ולבודד איזורים רגישים.

מומלץ לבחון את האבטחה במערכות מקוונות בשני שלבים. בשלב הראשון, יש לשקול באילו בקרות פיסיות ומנהליות להשתמש. בשלב שני, יש לבדוק אילו בקרות פיסיות מסופקות על ידי חומרת המערכת, התקשורת, התוכנה והמסופים. עם זאת, יש לזכור שבקרות טכניות, ללא בקרות מנהליות מקיפות ויעילות, הן חסרות תועלת. לדוגמה, אם פורץ יכול להכנס בקלות לחדר המחשב ולהגיע לעמדת המפעיל, סימן שהוא מחזיק במפתח לתיבת פנדורה.

פתרון בעיות אבטחה פיסיות ומנהליות נמצא באחריות ההנהלה. לעתים קרובות, קו ההגנה העיקרי במסופים מרוחקים הוא הסיסמה ומכשיר שמאפשר זיהוי של המשתמש. מכיון שהשימוש בסיסמאות אינו בטוח, הן יוחלפו בעתיד בשיטות זיהוי המשתמשות בחתימות, טביעת אצבעות וחתימת קול. בינתיים, כל עוד שיטות הזיהוי פגיעות וכל עוד צפוי שתהיינה תקלות בתוכנה ובמערכת, חשוב להשתמש בבקרות מנהליות ובתוכנה יישומית טובה ואמינה. בפרקים הבאים, במיוחד בפרק 6, נדון בנושאים אלה.

תוכנת מערכת ואמצעים טכניים אחרים עלולים להיות מורכבים וקשים להבנה. עם זאת, כאשר משתמשים בהם בצורה נכונה, הם עשויים לעזור בהפרדת תפקידים, להגביל את הנזק הנגרם על ידי שגיאות, לתפעל נתיבי ביקורת, לבדוק הרשאות ולספק אמצעי עזר אחרים לאבטחה. לרוב אין נוהגים להשתמש ברישום של השימוש במחשב, שמופק על ידי מערכת ההפעלה. הבעיה האמיתית היא שארגונים אינם מנצלים את פוטנציאל האבטחה המסופק על ידי הטכנולוגיה שקיימת בידם.

שאלות

4.1 ארגון עומד להכניס מערכת מקוונת למחלקה שעד לפני זמן לא רב השתמשה במערכת לעיבוד באצווה. מהן הבקרות שיש לשקול כדי למנוע מכל אחד להכנס למערכת?

4.2 ארגון מיקם את יחידת המחשב שלו במפלס הרחוב, בחדר המופרד מהמדרכה בחלונות גדולים. הדבר מאפשר לציבור הרחב לראות מן הרחוב את מסכי המסופים. מהן ההשלכות של מצב זה על האבטחה?

4.3 לארגון יש רשת תקשורת גדולה והוא חושש שמשתמשים לא מורשים יכנסו למשאבים המרכזיים דרך מסופים מרוחקים. הצע שיטות שיפחיתו את הסכנות.

4.4 בחר שני מחשבים שאתה מכיר והסבר, לגבי כל אחד מהם, את השיטות המשמשות להגנת הזיכרון ולהגנת האוגרים שמכילים נתונים להגנת הזיכרון.

4.5 בסעיף 1.4 נאמר שפונקציות האבטחה הבאות צריכות להיות באמצעי הנגד: (1) מניעה, (2) גילוי, (3) הרתעה, (4) אישוש, (5) תיקון, (6) מניעה. נתח את המאפיינים של המרכיבים הבאים ביחס לפונקציות אלו:

א. חומרה
ב. מערכות הפעלה
ג. רשתות תקשורת
ד. מסופים ומערכות מקוונות

4.6 לארגון יש יישום אחד, מתוך מאות, שהוא רגיש במיוחד. יישום זה רץ במשך שעתיים כל שבוע. הסבר כיצד אפשר להגן עליו בצורה מיוחדת.

4.7 מהן נקודות התורפה ומהם היתרונות של ציוד מרוחק, שממוקם בשטח משרדי פתוח ופועל בסביבת עיבוד מבוזר?

4.8 בחן את המדריכים במרכז המחשבים שלך וכתוב דוח על אבטחת החומרה ועל האבטחה המסופקת על ידי מערכת ההפעלה.

4.9 בקר במרכז מחשבים ומצא את האמצעים הקשורים למסופים מרוחקים ולמערכות מקוונות שממלאים את הפונקציות הבאות:

א. אבטחה פיסית
ב. בקרת כניסה
ג. טיפול בתקלות במסוף
ד. ניטור איומים
ה. בידוד

הצג את ממצאיך בדוח (משימה קבוצתית).

פרק 5

אנשים ואבטחה

אנשים הם מרכיב חשוב במערך האבטחה של מערכות מידע המבוססות על מחשב. יש לכך שלוש סיבות: הסיבה הראשונה היא שיש להגן על מערכות המידע מפני אנשים, כי הם יכולים לאיים על הארגון, כתוצאה מפעילות מכוונת, או לא מכוונת; הסיבה השניה היא שאנשים מהווים מרכיבים במערכות מידע, ולכן הם צפויים לאיום מבחוץ; לבסוף, אנשים יכולים לשמש כאמצעי נגד במהלך עבודתם השגרתית.

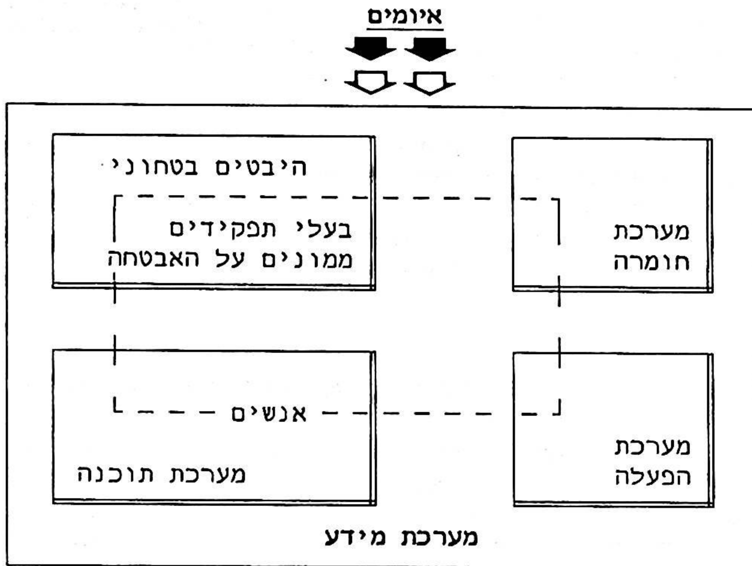
5.1 המעורבות של אנשים באבטחה

אנשים עושים טעויות, ללא קשר לאמינות המחשבים. הדבר עלול להתרחש במהלך השימוש במערכת, אך גם בזמן הבנייה של החומרה. בדומה, קווי ההגנה של מערכת מידע מתוכננים ונבנים על ידי אנשים ולכן הן עלולות להכיל טעויות, הגורמות לחשיפת המערכת. בכל מצב שקשור לאבטחה אפשר למצוא גרעין של פעילות אנושית. לצערנו, המרכיבים האנושיים של מערכת מידע המבוססת על מחשב אמינים פחות ופגיעים יותר, בהשוואה למרכיבי החומרה והתוכנה של מערכות. איום הנוצר על ידי עובד יכול להגרם מחוסר ניסיון, מחוסר יכולת, מהזנחה, או מפעילות זדונית, כמו גניבה או מרמה. לכן, על ארגון ומערכות המידע שלו להיות מוגנים מפני אנשים מבפנים ומפני אנשים מבחוץ.

אנשים, בדומה למערכות מידע, עלולים להיות קורבן לאיומים בדרכים רבות. דבר זה עלול לגרום לירידה בביצועים שלהם, ושל מערכת המידע שהם חלק ממנה. אנשים יכולים גם לשמש אמצעי אבטחה במהלך עבודתם. דוגמה מובהקת לכך הוא קצין אבטחת המידע, אבל אפשר לראות את האחראים לניטור ולבקרה של העבודה היומיומית באמצאות מערכות המידע בארגון, כחלק מאמצעי האבטחה. לדוגמה, מבקרים פנימיים ומנהלים של בסיסי נתונים פועלים כאמצעי אבטחה במהלך ביצוע המטלות השגרתיות שלהם. מצב זה מתואר בתרשים 5.1.

בסעיפים הבאים נדון בנושאים הבאים:

* הגנה מפני אנשים.
* הגנה על אנשים.
* שימוש באנשים כאמצעי אבטחה.



תרשים 5.1 בעלי תפקידים הממונים על הבטחה

5.2 הגנה מפני אנשים

המרכיב האנושי נמצא, בצורה כלשהי, בכל איום על האבטחה, בין אם הוא מכוון ובין אם אינו מכוון, ולכן ההגנה מפני אנשים חשובה מאוד. האנשים שמהווים איום יכולים להיות עובדי הארגון או אנשים מחוץ לו, שמועסקים על ידי ארגונים אחרים.

סעיף זה דן בעובדים של הארגון שמעורבים באופן ישיר ועקיף בניהול, בתכנון, בפיתוח, בתחזוקה, בתפעול ובשימוש של מערכות מידע ממוחשבות. בקטגוריה זו נמצאים מנהלים בכירים ומנהלי ביניים, מנתחי מערכות, תכניתנים, מפעילים ומשתמשים של המערכת. הם מהווים איום, מכיוון שהם עלולים לטעות בשוגג. למשל, הם עלולים להשמיט נתונים בקלט, לכתוב על נתונים בדיסק, לטעות בתכנות או בכתיבת המפרטים של המערכת. הם גם עלולים לבצע פעולות מכוונות, כמו גישה ללא הרשאה למידע חסוי,

הוצאה ללא רשות של מסמכים, דיסקים או סרטים מיחידת המחשב, או הכנסת "פצצת זמן" ("וירוס") לתוך תוכנית.

5.2.1 כללים לניהול נכון

רובם המכריע של העובדים ישרים ומבצעים שגיאות מעטות בלבד, אך על הארגון לדעת להתגונן בפני מיעוט של עובדים שיכולים לאיים על האבטחה בדרך של פעולות מכוונות. כדי להגן על עצמם, פיתחו הארגונים כללי ניהול, שהוכיחו את יעילותם הרבה במערכות מידע ידניות. כללי ניהול אלה יעילים גם במערכות מידע ממוחשבות והם עוזרים להתגונן גם בפני פעולות בשגגה (מרטין, 1973; FIPS 1980). כללי הניהול המומלצים הם:

(1) בדיקה ואיזון (check and balance): אלה יוצרים הגנה שמשמעותה הוא שפגיעה באבטחה תגרום נזק רק לאחר שהצליחה להתגבר על כמה קווי הגנה.
(2) הפרדת תפקידים ותחומי אחריות: אנשים שונים צריכים להיות אחראים על שלבים שונים בתהליכי העבודה.
(3) פיזור ידע: הידע על המערכת צריך להיות מפוזר בין אנשים אחדים.
(4) רוטציה בתפקידים: יש להעביר אנשים מתפקיד אחד למשנהו בפרקי זמן אקראיים.
(5) חופשות מאולצות.
(6) הגבלת האמצעים שנמצאים בטיפולו של עובד: יש לקבוע גבול עליון לסכום הכספי שיכול להמצא בטיפולו של עובד בסביבת עבודה פיננסית, ולהציב הגבלות דומות בסביבות אחרות.
(7) כניסה למידע על בסיס הצורך לדעת (Need To Know - NTK): ההרשאה למידע אינה צריכה להקבע לפי מפתח של דרגה או תקדים. יש להעניקה רק לאדם שצריך גישה למידע, לפי מהות תפקידו ומשימותיו.
(8) פיקוח של דרג בכיר יותר: כל עובד צריך לעבוד תחת פיקוח מתמשך של עובד מדרג בכיר יותר, שמכיר אותו ויכול לזהות אצלו תבניות התנהגות חריגות.

השילוב של הפרדת תפקידים עם בקרות ואיזון הוא תוצאה של גישה המוכרת מהעידן שלפני האוטומציה. גישה זו נמצאה יעילה מאוד גם במערכות ממוחשבות, כי היא עוזרת בהפחתת הסיכונים במערכות אלו. לדוגמה, הפונקציות של איסוף נתונים, הכנת נתונים, תפעול מחשב, תכנות מערכת, תכנות יישומים, הפצה של הפלט, ניהול של בסיס הנתונים, הרשאת כניסה לנתונים וביקורת פנימית - חייבות להיות נפרדות וללא חפיפה בין תחומי האחריות המוקצים לכל פונקציה. כאשר ממלאים דרישה זו, גורמים לעובד שרוצה לפרוץ למערכת לשתף פעולה עם עובדים אחרים מפונקציות

אחרות; במקרים מסוימים תדרש קנוניה בין צדדים רבים, כדי לפגוע במערכת. סביר להניח שעובד ינצל מערכת שאין בה צורך לשתף פעולה עם אחרים.

במערכות שנדרשת בהן רמת אבטחה גבוהה, חשוב לא רק להפריד תחומי אחריות, אלא גם לפזר את הידע על המערכת בין אנשים רבים ככל האפשר. ברור שהתפקיד של מנתח המערכות הופך יעד זה לבלתי ניתן להשגה. לכן, יש לשאוף לפיזור מלא של הידע רק במערכות שבהן מאוחסן מידע רגיש, שחשיבותו גבוהה במיוחד. לפי עיקרון זה יש לשים לב לפגיעות הנגרמת מהעובדה שחוברות הדרכה למשתמש ומפרטי תכנות של תוכניות נמצאים ללא הגנה מספקת.

חופשות תורמות לבריאות העובדים, אך הן גם מרתיעות עובדים ממעשי מרמה התלויים בנוכחותם המתמדת לשם שמירת הסודיות של הפגיעה. לרוטציה בתפקידים השפעה מרתיעה דומה על מעשי מרמה. במקרים רבים, הרוטציה בתפקידים אינה אפשרית וההגנה תהיה תלויה בפיקוח של עובד מדרג בכיר יותר. המקרים המתוארים בסעיף 11.2.2 מצביעים על הצורך בפיקוח גם על עובד ותיק, שניתן לכאורה לסמוך עליו.

מבלי להתייחס להצלחת הארגון ביישום כללי ניהול אלה, יש להכיר בעובדה שיש לכללים אלה גם מגבלות. תמיד יהיו אנשים שיהיה צורך לסמוך עליהם, כמו קצין הבטחון, או מנתח המערכות. לכן יהיו תמיד עובדים שיוכלו לפרוץ את ההגנה, אם רק ירצו בכך. למרות זאת, אין לתת אמון מלא בכל עובד ובמערכת מתוכננת היטב האבטחה תהיה תלויה באנשים מעטים בלבד.

5.2.2 כללי ניהול טובים שפותחו על ידי תעשיית המחשוב

תעשיית המחשוב הכירה ביתרונות של כללי ניהול טובים וכבר לפני חמש עשרה שנה יושמו באופן מקיף סטנדרטים לתיעוד. לתיעוד, להנחיות ולרשימות התיוג יש התפקידים הבאים (קורקורן ולייו, 1978):

* הם מפחיתים שגיאות והשמטות.
* הם תורמים לתקשורת טובה יותר בין מחלקות שונות.
* הם מקטינים ככל האפשר את הקשיים שבתיקון תוכנית.
* הם מבטיחים המשכיות בתפעול (יעד עיקרי של אמצעי האבטחה), במקרה של תקלה בציוד או בתחלופה של כוח אדם.

הדרכה היא פעילות עסקית נוספת שתעשיית המחשוב הכירה בחשיבותה. היא מאפשרת לעובד לבצע את המטלות היומיומיות שלו ונחשבת לנורמה. אבל הדרכה לחובות הקשורות באבטחה אינה

נפוצה עדיין. קשה להניח שעובדים יוכלו לעזור באופן פעיל באבטחה, ללא הדרכה וללא עידוד של ההנהלה. על ההדרכה לכסות שלושה נושאים:

(1) הדרכה ותרגול של משימות מסוימות: אלו הן המיומנויות שדרושות לתפקידים ספציפיים שקשורים באבטחה, כמו המשימות שיש לבצע במקרה של אש.

(2) הגברת המודעות לאבטחה: קיימים חובות מוגדרים שקשורים באבטחה, אך יש להוסיף עליהם חינוך של העובדים לאבטחה, על ידי הדרכה בנושאים כמו מדיניות החברה לגבי אבטחה, פרטיות המידע ושלימותו, התרומה של כל עובד לאבטחה והשפעת עיכובים ושיבושים בעיבוד על פעילות הארגון.

(3) תגובה לאירועים חריגים שיש להם השלכה על האבטחה: אירועים חריגים, כמו ניסיון גישה לא מוצלח למחשב ולחדר המחשב, או תקלה במערכת הכיבוי, מתרחשים מדי יום בארגונים. הם כוללים כל אירוע הקשור לאבטחה, שסותר את מדיניות האבטחה, שלא ניתן להסביר אותו, או שהוא יוצא דופן. אם לא מתכוונים להתעלם מאירועים אלה, יש לקבוע נוהל דיווח לאדם שהתמנה לצורך זה.
יש לשמור על סודיות המדווח, כדי לא ליצור תווית של הלשנה. יש להדגיש את חשיבות הדיווח על אירועים חריגים בתוכנית להגברת המודעות, עם זאת, צריך להכיר בכך שעובדים לא ידווחו על כל האירועים, מכיוון שבחלקם מעורבים חברים שלהם או חברים לעבודה. דיווח על אירועים חריגים וטכניקת האירוע הקריטי נסקרים בהרחבה בסעיף 8.5.

5.2.3 מנתחי מערכות

מנתחי המערכות נמצאים בעמדה עדיפה בארגון, כי עבודתם מאפשרת להם לקבל מידע מפורט על היבטים רבים של פעילות הארגון. הם חופשיים להכנס לכל מקום בארגון ולהכיר כל אחד מהעובדים ואת הנוהלים והנתונים. מידע זה דרוש למנתח המערכות כדי לבנות מערכת שתתאים לדרישות המשתמש ושתכיל את דרישות האבטחה, כמתואר בפרקים 6, 7 ו-8.

יש להתייחס לאבטחה בכל שלב בתהליך התכנון; יש ללמוד את הנושא בניתוח המקדים ולפתח אותו בכל שלבי הפיתוח, כדי שהפתרון יתאים גם לדרישות עתידיות. העבודה של מנתח המערכות היא הבסיס לכל מה שיבוא אחריו, ולכן חשוב מאוד שהעבודה תנוהל ותבוקר באופן שיסיר, או שיקטין ככל האפשר, איומים

מכוונים ושאינם מכוונים מצד מנתחי המערכות עצמם. איומים לא מכוונים (ראה טבלה 5.1) נגרמים מהאופן שבו מבצע מנתח המערכת את התכנון. לגבי איומים מכוונים, חייב להיות למנתח המערכות מניע לגרום פגיעה באבטחה. מניעים נפוצים יכולים להיות תאוות בצע, כעס ואחרים, כמו גאווה מקצועית, או בורות, כמתואר במקרה המובא בסעיף 11.3. מניע וידע על הארגון לבדם אינם מספיקים כדי לגרום פגיעה באבטחה. חייבות להיות נסיבות שיאפשרו זאת, כלומר פגיעויות, לפני שהמניע הופך לאיום ולפני שהאיום הופך לאובדן (ראה תרשים 5.2). זו הסיבה ליעילותם הרבה של כללי הניהול, שנסקרו בסעיף 5.2.2, כאמצעי אבטחה נגד פגיעות מכוונות ושאינן מכוונות באבטחה. שלוש טכניקות רלוונטיות גם לגבי צוותים לניתוח ותכנון מערכות:

(1) הפרדת תפקידים: מנתח המערכות לא יהיה מעורב בשום צורה בתכנות ובהפעלת המחשב.
(2) נוהלי עבודה רשמיים של הארגון: עבודת הפיתוח חייבת להיות מאושרת על ידי המשתמשים ועל ידי הנהלת יחידת המחשב. יש לקבוע נקודות ביקורת בשלבי התכנון השונים, כדי לקבוע עם התכנון מתקדם בהתאם לציפיות. נוהלים אלה יעזרו לגלות טעויות והשמטות ולהרתיע מנתחי מערכות מלהכניס שגרות הרסניות, או כאלו שיתמכו במעשי מרמה.
(3) פיקוח קבוע וצמוד של עובד מדרג בכיר יותר על עבודת מנתח המערכות.

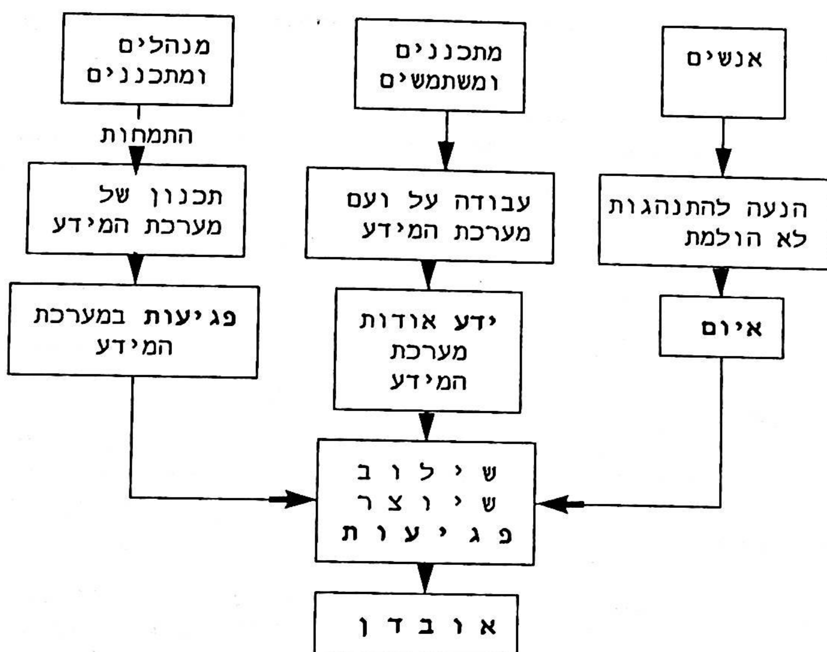
5.2.4 תוכניתני יישומים

השימוש בהפרדת תפקידים, בסטנדרטים, בתיעוד טוב ובשיטת הרשאה יעילה חשובים בשלב התכנות, בדיוק כמו שהם חשובים בשלב הניתוח והתכנון. יש לצמצם ככל האפשר את סכנת השגיאות או ההשמטות שעוברות מהפיתוח לתוכניות פועלות. תוכניות לא תקינות עלולות לפגוע בכל ההיבטים של האבטחה, כלומר בשלימות, בזמינות ובסודיות. במובן זה, העבודה של תוכניתן חשובה מזו של מנתח המערכת. למרבה המזל, אפשר לצמצם מאוד את ההשפעה של איומים מכוונים ושאינם מכוונים על ידי ניסוי מקיף, עוד לפני שהתוכניות מועברות לייצור. יש להשלים את הניסוי בבדיקה ידנית, בתהליך סקירה מובנה (structured walkthrough) ובבדיקה על ידי עמיתים (peer review).

טבלה 5.1 מניעים, פגיעויות ואיומים הנוצרים בזמן הניתוח, התכנות והתפעול

מניע או סיבה לפעולה	פגיעויות	איומים
1. <u>פעולות לא מכוונות</u> חוסר נסיון או ידע מצב פיסי, כמו עייפות או עומס יתר בעבודה מצב רגשי	השמטות וטעויות בתכנון תיעוד מועט קיצורים בתכנון שביעות רצון בקשר לרמת האבטחה עבודה לבד בשעות לא מקובלות בקרה מועטה על צוות הניתוח	1. <u>לא מכוון</u> טעויות והשמטות בקלט כתיבה על נתונים באמצעי הגיבוי
2. <u>פעולות מכוונות ולא מכוונות</u> הסביבה הארגונית שבה מבוצע, למשל, ניתוח המערכת. אין מתודולוגיית פיתוח		2. <u>מכוון</u> הצצה למידע רגיש חבלה גניבה של משאבים שינוי ישיר של קובץ או תוכנית
3. <u>פעולות מכוונות</u> רווח אישי גאווה מקצועית כעס נקמה בורות		

תיקון תוכניות מהווה סיכון גדול, מכיוון שהתוכניות נמצאות במצב זמני (ראה גם פרקים 6 ו-8). במהלך התיקון קיימות אפשרויות רבות לטעויות, ולכן יש לקבוע וליישם נוהלי תחזוקה מפורשים למניעתן. לדוגמה, יש לבצע תיקון לעותק של התוכנה ולנסות אותה עם נתוני ניסוי בפיקוח ובהגנה של מערכת ההפעלה, כדי להבטיח שתוכניות חיות ונתונים אמיתיים לא יפגעו. על צוות תוכניתנים בכיר לפקח על מתכנתים אחרים, כדי להבטיח שכל נוהלי התיקון בוצעו.



תרשים 5.2 קשר בין אנשים לבין אובדן מידע

לסיכום, ארבעה עקרונות אבטחה בניהול צוותי מתכנתים:

(1) יש לחלק תחומי אחריות בין מתכנתים שונים, כדי שאף אחד לא יחזיק כמות מידע שתאפשר לו לבצע מעשה מרמה מבלי להסתכן בחשיפה.
(2) יש להעביר תוכניות לסביבת הייצור, רק לאחר שעברו ניסוי מקיף ותיעודן נמצא מתאים.
(3) אין לאפשר לתוכניתנים גישה למידע רגיש, לבד ממקרים מיוחדים, כמו תקופת אישוש לאחר תקלה, ורק תחת פיקוח הדוק.
(4) תוכניתנים צריכים להיות מודעים שהעבודה שלהם צפויה לפיקוח ולביקורת (מרטין, 1973).

5.2.5 עובדים המעורבים במערכת ההפעלה

פעילויות התפעול כוללות קליטת נתונים, הסבת נתונים ועיבוד, ייצור ופיזור של הפלט. לכן, פגיעה באבטחה עלולה לפגוע

בשלימות הנתונים, בסודיותם ובזמינות של השירותים. מצבים זמניים פגיעים במיוחד, כמוסבר בפרק 8. בתפעול היומיומי עלול להתרחש מצב כזה כאשר נתונים נמצאים במעבר בין מחלקות ובין אתרים המפוזרים מבחינה גיאוגרפית. יש להכיר בסכנות שבמצבים אלה ולמנות אדם מהימן שיהיה אחראי על המידע במעבר. בטבלה 5.2 תמצא איומים נוספים ואת אמצעי הנגד המתאימים להם. אבטחה בזמן התפעול תידון שוב בפרק 7.

יש לזכור שמפעיל אחד שעובד ללא השגחה יכול לעקוף את מערכת האבטחה הטובה ביותר. פקודות מסוימות של מערכת ההפעלה (ראה סעיף 11.3) יכולות לעזור למפעיל למסך את פעולותיו. לכן, יש להפעיל בקרה נפרדת על חברי צוות התפעול, מכיוון שביכולתם להשפיע על המערכת ועל נתיבי הביקורת. בקרה תושג על ידי מבנה ארגוני נכון ועל ידי שימוש בנוהלים אמינים ובסטנדרטים (סקווירס, 1980).

טבלה 5.2 איומים ובקרות בפונקצייה התפעול

איום	פגיעה ב-	אמצעי נגד
פגיעה בנתונים בגלל: * טיפול חסר אחריות באמצעי האחסון * תקלה * עיבוד לא נכון * עיבוד כפול	שלימות הנתונים	עותקי גיבוי, רישום פעולות, נוהלי הפעלה, סיכומי ביקורת
מסמכים פיננסיים (כמו המחאות) אבדו, או שהונחו במקום לא נכון	שלימות	בדיקות ובקרות (על ההנפקה, על השימוש, על החזרות ועל חיובים)
שימוש שלא כדין במשאבי המחשב	זמינות של שירותים	פיקוח על העובדים ועובד אל יורשה לעבוד לבד; רישום פעולות על ידי מערכת ההפעלה
מישק לנתונים: * הצצה ללא ההרשאה של צופים מזדמנים * דוחות שאינם בשימוש מגיעים למי שאיננו מורשה	סודיות	תפעול טוב, פיקוח, הגבלת כניסה, הפלט מטופל בידי מספר מועט של אנשים. גריסה של הפלט הרגיש שאיננו בשימוש

5.2.6 משתמשים של מערכות המידע

בארגונים שונים סבורים שהאבטחה חיונית רק בתוך יחידת המחשב ובסביבה הקרובה אליה, ואין רואים במשתמשי הקצה מוקד לפגיעויות שזקוק להגנה. לכן, יחידות מחשב המוגנות בצורה הטובה ביותר נבנות במחלקות של משתמשים שאינן מוגנות כלל. משתמשים יכולים לקבוע אם תוכנית האבטחה תצליח או תכשל. האירועים שמוצגים בסעיף 11.2 מראים כיצד מחלקות המשתמשים עלולות להיות פגיעות מאוד למעשי מרמה. המשתמשים מכירים את הנוהלים והם עלולים לסייע בכך לביצוע מעשה מרמה. לכן, המשתמשים צריכים להיות תחת ניטור, בקרה וביקורת, בדומה לצוות התפעול של יחידת המחשב.

5.2.7 עובדים של ספקים

מערכות מידע המבוססות על מחשב תלויות בשירותים של ספקים. תכנון טוב של ההנהלה עשוי להקטין למינימום את האיומים מצד עובדים חיצוניים (ראה גם טבלה 5.3).

טבלה 5.3 האיומים שמציבים עובדים חיצוניים

שירות או איום לשירות	פגיעה ב -	אמצעי נגד
תחזוקה של המחשב ושל ציוד חיוני אחר	סודיות של נתונים, זמינות של שירותים	בקרות כמו לצוות התפעול של הארגון המארח
ספקים מעכבים אספקה * במכוון (למשל, במהלך שביתה) * לא במכוון (למשל, בגלל תקלה בייצור או במכונות)	זמינות של שירותים	מלאי מספיק של חומרים וציוד חיוניים
אספקת החשמל שמופסקת בטעות על ידי קבלנים של עבודות עפר, או על ידי חברת החשמל: * אספקת חשמל רציפה * אספקת מתח בגבולות מותרים	זמינות של שירותים	מערך גיבוי לאספקת חשמל כמו למשל, גנרטור ו/או UPS

5.3 מדיניות החברה לגבי גיוס, הערכה ופיטורין של עובדים

גורמים שונים של ניהול כוח אדם מעורבים בתוכנית ההגנה על מערכות מידע ממוחשבות. הסטטיסטיקה מלמדת שעובדים ממורמרים, משועממים או לא ישרים אחראים לחלק גדול מהפגיעות באבטחה. אפשר להקטין למינימום את הסכנות מצד העובדים בעזרת ניהול נכון של כוח אדם, המבוסס על מדיניות ברורה של החברה, שכוללת:

(1) נוהלים רשמיים לגיוס, להערכה ולפיטורין של עובדים.
(2) הכרה בהשפעה של מורל העובדים על ביצועיהם.
(3) תוכנית הדרכה שתשפר את הביצועים ושתקדם את האבטחה.

במקומות רבים נהוג לבצע בדיקות רקע למועמדים, אך הצלחתן מוטלת בספק, מכיוון שרוב פשעי המחשב בוצעו על ידי אנשים שזו עבירתם הראשונה (ראה גם פרק 11). במהלך הגיוס קל למדי לקבוע אם מועמד למשרה מתאים מבחינה טכנית, אך קשה הרבה יותר לקבוע אם הוא מתאים לארגון, כלומר, אם הוא האדם המתאים למשרה זו.

לאחר שגוייס עובד, יש לשים לב לביצועיו ולמוראל שלו, לטובתו הוא ולטובת הארגון שהוא משרת בו. באופן כללי, כל המשימות המוטלות על עובד חייבות להיות בכתב. אפשרי לעשות זאת במערכות מידע, כי התיעוד והמדריכים להפעלה מפורטים ואף זמינים בדרך כלל. אפשרויות ההעסקה חייבות להעניק סיפוק אישי וקידום בעבודה. נושא זה חיוני, אך נתון במחלוקת. בעיות תעסוקתיות, כמו אי ניצול של כישורי העובד, יביאו לביצועים נמוכים ואפילו לפגיעה באבטחה. מסיבה זו ואחרות, יש לצפות שעובדים יתפטרו או יפוטרו מעבודתם. לארגון חייבים להיות נוהלים מתאימים לכל מצב של הפסקת עבודה, המייצגת דוגמה נוספת למצב זמני שיש בו סיכון גבוה לפגיעה באבטחה. לאחר שעובד קיבל הודעה מוקדמת על פיטורין יש לבצע את הפעולות הבאות:

* לאסור עליו, בהקדם האפשרי, את הגישה למקומות רגישים.
* לוודא שיחזיר פריטים שונים, כמו מדריכים לתפעול, מפתחות ותגי זיהוי.
* לבטל ולהעביר את כל הסיסמאות וההרשאות הקשורות למערכות המידע, שהיתה לו נגישות אליהם.
* להחתים אותו על הצהרה של שמירת סודיות, לגבי תוכניות ונתונים שהיתה לו גישה אליהם.

פיקוח נכון ומדיניות ברורה בנושאי כוח אדם חשובים וחיוניים, כמו שיטות גיוס טובות. מדיניות החברה צריכה להיות כזו שהעובדים יידעו מה מצופה מהם מרגע התחלת עבודתם. יש להעביר

להם תוכנית להגברת מודעות האבטחה ולהסביר להם את משימות האבטחה שהם נדרשים לבצע. עליהם להיות מודעים לעונשים המשמעתיים שיוטלו על אלה שלא ימלאו אחר דרישות האבטחה. יש להעניש את מפירי ההוראות באופן הוגן ולפרסם זאת ברבים, כדי להרתיע עובדים אחרים.

5.4 הגנה של עובדים

עובדי החברה הם מרכיבים של מערכת מידע, כנראה אחד המרכיבים הפגיעים ביותר. לכן, על הארגון לדאוג שעובדיו לא יהיו צפויים לנזק בריאותי, לפציעה (מתקיפה), לסחיטה ולהתרנות. לדוגמה, אסור שמידע על עובדים, שנמצא ברשומות הארגון, יגיע לאנשים שאינם מורשים לגשת אליו, מכיוון שזו תהיה פגיעה בפרטיות של העובדים. קיימים סוגים רבים של עובדים המעורבים בתפעול, בתחזוקה ובתכנון של מערכות מידע המבוססות על מחשב. בכלל זה מנהלי יחידות מחשב, מנתחי מערכות, תוכניתנים, מפעילים, משתמשים ומהנדסי תחזוקה. אנשים אלה הם בעלי ערך רב לארגון ובמקרים מסוימים מהווים נכס שאינו ניתן להחלפה. על ההנהלה ליצור סביבת עבודה שתגן על עובדים אלה, לטובתם הם ולטובת החברה.
סביבה מתאימה נוצרת על ידי תנאי העסקה טובים ובטחון פיסי. תנאים טובים עוזרים להפחית חולי, העדרויות, תחלופת עובדים ובעיות של יחסי עבודה. הם גם מגבירים את היעילות של שירותי המחשוב ותורמים לסיפוק בעבודה. בטחון פיסי (ראה פרק 2) כולל הגנה על אנשים מאש, מפורצים (כמו מחבלים), מהתפוצציות ומאסונות טבע, כמו רוח, ברקים והצפות.

5.5 עובדים כאמצעי הגנה

5.5.1 מנהלים בכירים ומנהלים מדרג ביניים

כל בדיקה תוביל למסקנה שהאחריות לאבטחה נמצאת בידי ההנהלה הבכירה. עליה מוטלת האחריות לפתח ולקדם
(1) אסטרטגיית אבטחה משופרת לארגון
(2) מדיניות שתהפוך את האסטרטגיה הזו למציאות.

כדי להשיג זאת נדרשת תמיכה טכנית של עובדים בכל רמות הארגון. לחלק מבעלי התפקידים בארגון, כמו קציני אבטחת מידע, מבקרים פנימיים, מנהלי בסיס הנתונים ומנהלים מדרג ביניים יש חזיקים בחובות מיוחדים שקשורים לאבטחה.

מנהלים בכל הרמות חייבים להכיר את הכפופים להם, כדי שיוכלו לגלות שינויים בהתנהגותם. כל שינוי כזה עלול להוביל לפגיעה באבטחה. המתאימים לתפקיד זה הם מנהלים מדרג בינוני, בעיקר כגורם שיעודד עובדים לדווח על אירועים חריגים. למנהלים מדרג ביניים תפקיד מרכזי בפעילות העסקית, היומיומית ולכן - גם באבטחה.

5.5.2 קצין אבטחת המידע

יחידת מחשב גדולה יכולה להעסיק קצין אבטחת מידע במשרה מלאה. תפקידו לדווח להנהלה, לפקח, לבדוק שהעובדים ממלאים אחר נוהלי האבטחה ולעזור במניעה ובגילוי של פגיעות באבטחה. קצין אבטחת המידע ינהל בדיקות תקופתיות, כמאמץ משותף של הארגון כולו. כל בדיקה תתבסס על רשימת תיוג מאושרת, שפותחה על ידי גורם מוסמך (ווריגג, 1978; 1979, AFIPS). קצין אבטחת המידע אינו מתפקד כחוקר. תפקידו העיקרי הוא לבנות סביבה בטוחה, שבה העובדים מודעים לחובותיהם ואינם מתפתים למעשים חריגים, מחשש שמא יתגלו.

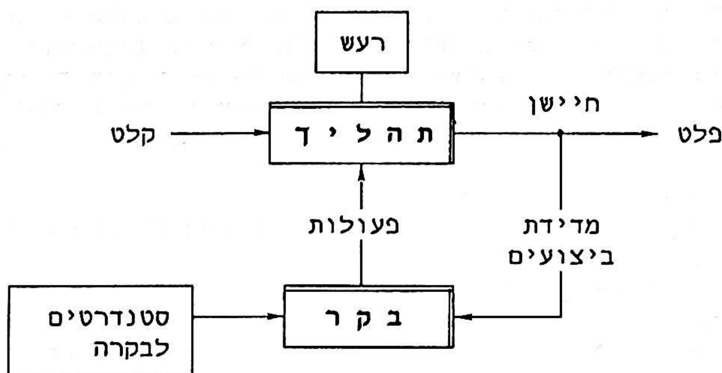
5.5.3 המבקר הפנימי

אמצעי אבטחה הם צורה ייחודית של בקרה, שהתקיימה לאורך השנים באמצעות מבקרים חיצוניים ופנימיים בארגון. למערכת בקרה, שמוצגת בתרשים 5.3, יש מספר מנגנונים שתפקידם:

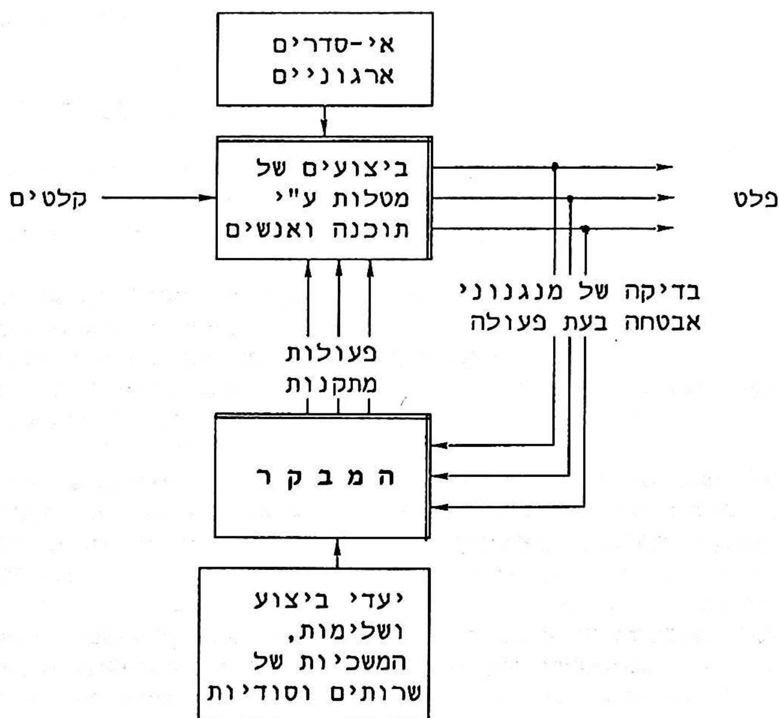
* לקבוע סטנדרטים או מטרות.
* לרשום את הביצועים.
* לבצע השוואה תמידית בין הביצועים לבין המטרות.
* לנקוט בפעולה מתאימה במקרה של תקלה, כדי להחזיר את הפעילות לסטנדרט שנקבע לה.

המטרות באבטחת מידע: שלימות, זמינות של שירותים וסודיות. כדי לבחון את אמצעי האבטחה, בודק המבקר את אמצעי האבטחה, מעריך אותם ומדווח על התוצאות. היתרונות בעבודת המבקר הפנימי הן:

* מעמדו סמכותי, הוא המדווח להנהלה הבכירה ובדרך כלל, הוא חופשי ממעורבות ביחסים מחלקתיים, או בין-מחלקתיים.
* הוא בעל ניסיון בתחום הביקורת.
* האחריות שלו כוללת את כל החברה, כולל מערכות המידע.



תרשים 5.3 (a) בקרה בעזרת משוב



תרשים 5.3 (b) המבקר כבקר אבטחה

ארגונים תלויים במידה רבה במערכות מידע המבוססות על מחשב. לכן, מתפקידו של המבקר להרחיב את שיטות הביקורת המסורתיות, שפותחו למערכות ידניות, כדי שיקיפו את כל שלבי הפיתוח של מערכות המידע בארגון.

הביקורת כוללת סקר של:

(1) השיטות ותהליכי התכנון והפיתוח של מערכות חדשות.
(2) השיטות והנהלים לביצוע שינויים במערכות.
(3) הבקרות המבטיחות שהבקרות התיאורטיות ממלאות אחר דרישות ההנהלה והחוק.
(4) הבקרות המבטיחות את אמינות התפעול.
(5) הבקרה הכוללת של המערכות, שמתפקידה להעריך את יעילותן בהפקת מידע מדויק.

לסיכום, תפקיד המבקר להבטיח שמספר בקרות האבטחה שהוכנסו למערכת הוא כנדרש, ושקיימת אפשרות לנהל נתיב ביקורת במהלך פעולת המערכת. יש להבטיח שהמערכות המטפלות בהנהלת חשבונות ובנושאים כספיים אחרים, יפעלו על פי כללים שיעילותם הוכחה לאורך השנים.

5.5.4 מנהלן בסיס הנתונים

למערכת לניהול בסיס נתונים בעיות מיוחדות, מכיוון שארגונים שונים משתמשים בתוכנה שאופן פעולתה מוכר גם לאנשים מחוץ לארגון, שעלולים להיות גורם סיכון. יש למנוע מאנשים חיצוניים לגישה חופשית לסביבת בסיס הנתונים, לסיסמאות ולכלי השליטה עליו. שילוב נתונים השייכים למספר רב של משתמשים יוצר בעיות מיוחדות ולכן יש לנקוט בצעדים הבאים, כדי לספק הגנה לנתונים:

* למשתמשים תהיה גישה רק לנתונים שלהם, תוך שימוש בבקרות הדוקות, כמו סיסמאות, שנסקרו בפרק 3.
* בסיס הנתונים יהיה מבוקר באופן קבוע (על ידי מנהלן בסיס הנתונים), כדי להבטיח את שלימות הנתונים.
* קבצים ונתונים יסווגו, במידת הצורך, כסודיים.
* המשתמשים יחזיקו בהרשאות וזכויות גישה, בהתאם לדרישות עבודתם, על בסיס הצורך לדעת (NTK).

מורכבות המבנה והתפעול של המערכות לניהול בסיס הנתונים מחייבת להפקיד את הבקרה באחריותו של עובד אחד, מנהלן בסיס הנתונים. עליו לקיים את הבטיחות והיעילות של פעולת בסיס הנתונים. אך הכוח שניתן בידיו מהווה יתרון וחסרון כאחד

(ווטן וטרני, 1984). עמדה זו נועדה לשיפור הבקרה, אולם יכולתו של מנהלן בסיס הנתונים לנטר פעילויות, כמו הוספות, ביטולים ושינויים, מאפשרת לו לפתח טכניקות שיעקפו את הבקרות הקיימות. לדוגמה, אדם זה יכול לשנות את בסיס הנתונים מבלי ליידע איש, כי הוא עצמו מהווה את מנגנון הבקרה של פעילות זו. אפשר להתגבר על בעיות של הפרדת פונקציות בעזרת כללי הניהול שתוארו בסעיף 5.2.1:

(1) רוטציה בתפקידים: יש להחליף את האדם הנמצא בתפקיד מנהלן בסיס הנתונים באופן קבוע ובפרקי זמן אקראיים.
(2) פיקוח על ידי עובד מדרג בכיר יותר.
(3) רישום של כל בקשת גישה של מנהלן בסיס הנתונים לבסיס הנתונים לשם בדיקה, כך, בשלב מאוחר יותר יוכל המבקר לעקוב אחר תהליכי העבודה, לצורך גילוי של ביצוע פעולות לא חוקיות.

5.6 סיכום

לאנשים תפקיד חשוב בכל הפגיעויות הקשורות לאבטחה. פגיעה במערכת המידע עלולה לגרום לכך שפעולות מכוונות ולא מכוונות יגרמו לאובדנים. הארגון צריך להגן על כל מערכות המידע מפני אנשים. אפשר להשיג זאת על ידי בקרות מקיפות ומשמעותיות. כדאי ליידע לעתים קרובות את העובדים על אמצעי האבטחה ולהסביר להם את תרומתם, ותרומת חבריהם לעבודה, ביצירת סביבה בטוחה, שבה הגנות עשויות להרתיע תוקף פוטנציאלי.

עובדים מסוימים מהווים מרכיבים חיוניים במערכות המידע ולכן יש להגן עליהם, כמו על רכיבים אחרים של המערכת. ללא קשר להצלחת הארגון ביישום נוהלים שיגנו על העובדים ועל מערכת המידע מפני העובדים, יש לתת אמון באנשי מפתח שיכולים לעקוף את האבטחה. אלה כוללים את מנתחי מערכות ואנשים אחרים שמחזיקים בחובות הקשורים לאבטחה ואף משמשים בעצמם אמצעי נגד. אין צורך לתת אמון בכל עובד. ארגון המנוהל היטב ידאג לצמצם את מספר האנשים שעבודתם לא תבוקר.

שאלות

5.1 נסה לזהות, מחוץ למקום לימודיך, או מחוץ לארגון שבו אתה עובד, אנשים שמהווים איום על מערכות מידע המבוססות על מחשב, ולכן הם מהווים איום לארגון. הסבר במה מתבטא איום זה ומהו אמצעי הגנה שאפשר להפעיל נגדו.

5.2 מדוע העיקרון של הפרדת תפקידים עוזר להבטיח את שלימות

התנועות הפיננסיות במערכות מידע?

5.3 רצוי להעסיק מפעילי מחשב שאין להם ידע בתכנות. הסבר את היתרונות והחסרונות שבגישה זו.

5.4 חסרונות רבים לרוטציה בתפקידים. הסבר.

5.5 כדי לעמוד בדרישה של פיזור ידע, חשוב שבכל פרוייקט פיתוח יהיו לפחות שני מנתחי מערכות. הסבר.

5.6 נתח את שני המקרים שמתוארים בסעיף 11.2 וציין איזה מבין כללי הניהול הטובים לא הופעל.

5.6 ההגנה על כח-אדם דורשת תנאי העסקה טובים. הסבר מהם "תנאים טובים" וכיצד הם מתקשרים לאבטחה.

5.8 המבקר הפנימי צריך לבדוק רק את הבקרות הקיימות במערכות הפעילות ולא לבזבז את זמנו על שיטות המשמשות לפיתוח של מערכות חדשות. הסבר את היתרונות והחסרונות שבגישה זו.

5.9 (א) פרט את המשימות שבאחריות קצין אבטחת המידע.

(ב) ביחידת מחשב קטנה עם שניים או שלושה תוכניתנים/מנתחי מערכות:

(1) על מי צריכה להיות מוטלת האחריות לאבטחת מידע?

(2) האם קיימים תפקידים של קצין הבטחון שלא ניתן ליישם במצב זה?

5.10 לשני קציני אבטחת מידע ניסיון של עשר שנות עבודה בארגון. הם מציעים את עצמם לעבודה בארגונך. גילם, כישוריהם, ניסיונם, המלצותיהם ויכולת האלתור שלהם נראים דומים. ההבדל האמיתי ביניהם הוא בכך שקצין הבטחון הראשון, CSO1, גילה במשך עשר שנות עבודתו אנשי מחשב ועובדים רבים אחרים שמנצלים לרעה את שירותי המחשוב. לעומתו, CSO2, גילה במשך עשר שנים רק שתי פגיעות באבטחה, שאחת חשובה יותר והשניה חשובה פחות. במקרה הפחות חשוב המליץ CSO2 שהגורם המעורב יוזהר, אך יישאר בחברה. במקרה היותר חשוב פוטר העובד, מבלי שננקטו נגדו צעדים משפטיים. מנהל כח-אדם שלך ממליץ שקצין אבטחת המידע השני יתקבל לעבודה. מה לדעתך היו השיקולים של מנהל כח-אדם והאם יש לדעתך סיבות להעדפת קצין הבטחון הראשון?

5.11 באילו שיטות אפשר להבטיח את אמינות עבודתו של תוכניתן יישומים? ציין נקודות חשובות לבקרה של תוכניתן היישומים.

5.12 אבטחה תלויה ביושרם של אנשים. לכן, ארגון צריך להתרכז בנוהלי גיוס קפדניים. כך ניתן להתעלם מכללי נוהל והנחיות טכניות שהומלצו, מכיוון שאין בהם ערובה לאבטחה. מהי דעתך על טענה זו?

5.13 באילו אמצעי הגנה אפשר להשתמש כדי להפחית את הסכנה מפני תוכניתנים לא ישרים שיכולים להכניס פגיעויות בתוכניות?

פרק 6

שילוב בקרות אבטחה בשלבי הפיתוח של מערכת התוכנה

פרק זה דן בצעדים שיש לנקוט כדי להבטיח שאמצעי אבטחה ישולבו במערכות של תוכנה יישומית בשלבי העיצוב, התכנון, התכנות וההפעלה שלהן. בתהליך זה, האחריות למדיניות האבטחה היא בידי הנהלת הארגון, משתמשי הקצה והמבקרים הפנימיים, אבל התכנון המפורט וההתקנה של אמצעי האבטחה נתונים בידי מתכנני המערכת.

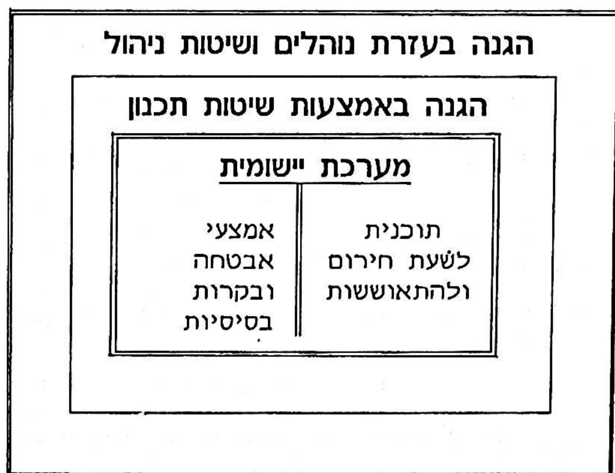
6.1 הנהלה, משתמשים ואמצעי הגנה

המערכת מידע כוללת את האנשים שמשתמשים במערכת, הצוות הטכני שמפעיל אותה, החומרה והתוכנה. מרכיב חשוב נוסף הוא התוכנה היישומית שנוצרת על ידי תוכניות מחשב, שהן "לב" מערכת המידע. כדי שהתוכנה היישומית תפעל ביעילות, יש להתקין מנגנוני אבטחה ובקרות בתוך התוכנה ובמישק שבינה לבין מרכיבים אחרים של מערכת המידע. לכל אמצעי הגנה, החל מבקרות טכניות מתוחכמות ועד לבקרות פשוטות ונפוצות, תפקיד משלו. יש לזכור שעד כה דווח על פגיעות מעטות בלבד בהגנת החומרה, אך דווח על אירועים רבים שבהם עקפו אנשים בקרות מנהליות וחדרו למערכת, מבלי שהבקרות הטכניות יכלו להגיב. על האבטחה להיות מקיפה ולהיות חלק אינטגרלי בפיתוח המערכת ובתפעולה. בפרק 1 ובטבלה 6.1, נראה שלמערכות השונות צרכי אבטחה שונים. לכן, על אמצעי האבטחה לשקף את צרכי המערכת ולהתאים לרגישות המידע המעובד על ידה ורגישות התמיכה שלה לפעילות העסקית.

היעד של תכנון טוב הוא בניית תוכנה יישומית בטוחה. לשם כך, יש להשתמש בגישה שיטתית שלוקחת בחשבון את הסביבה הארגונית שבה מתבצע עיצוב התוכנה. גישה זו צריכה לכסות את תכנון הפיתוח, שיטות העיצוב ובחירת מנגנוני האבטחה. בתהליך זה מעורבים אנשים רבים, ביניהם ההנהלה, משתמשי המערכת, מבקרים ואנשי מחשב מקצועיים. בסעיפים הבאים נתייחס לארגון שבו מתבצע עיצוב המערכת ולמתודולוגיית תכנון האבטחה. לבסוף, יוצגו כמה בקרות בסיסיות שאפשר להתקין בתוך התוכנה היישומית, או במישק שלה. בתרשים 6.1 מוצגים הקשרים בין נושאים אלה.

טבלה 6.1 איומים ומערכות מידע טיפוסיות

מערכת המידע		איום עיקרי	יעד אבטחה עיקרי
סוג	דוגמאות		
ניהול נכסים וניהול פיננסי	שכר, ניהול מלאי וקניות	פעולות מכוונות ולא מכוונות	שלימות
תמיכה בפעולות עסקיות	CAD, תמיכה במערכות רפואה	פעולות לא מכוונות	שלימות
קבלת החלטות אוטומטית	רישום מלאי, קביעת לו"ז לתחזוקה	פעולות לא מכוונות	שלימות קפדנית



תרשים 6.1 אמצעי אבטחה באמצעות שיטות תכנון, נוהלים ארגוניים ותוכנה יישומית

6.2 ההנהלה והסביבה הארגונית

בחירת בקרות אבטחה תלויה בגורמים רבים, מעבר לרגישות הנתונים המעובדים והתרומה של המערכת לפעילות העסקית. לפגיעויות הנוצרות בסביבה שבה פועלת המערכת השפעה ניכרת על בחירת אמצעי האבטחה ועל יעילות התפעול של המערכת. גורמים רבים מעצבים את הסביבה שבה פועלת מערכת המידע, בכללם:

* מדיניות האבטחה של החברה.
* כללי ניהול המשמשים את ההנהלה לבקרה על פיתוח מערכות מידע.
* שימוש בכללי ניהול נכונים, שהוכיחו את יעילותם לאורך השנים.

מערכת המידע תהיה בטוחה רק אם היא תהיה חלק מארגון שיש לו גישה חיובית לאבטחה. לארגון צריכה להיות מדיניות אבטחה פנימית וחיצונית, שבה מודעים העובדים לאחריות המוטלת עליהם במניעת מידע מגורמים לא מורשים (סקווירס, 1980). בדומה, ארגון צריך להשתדל ליצור סביבת ניהול לפרויקטים של פיתוח מערכות. ניהול פרויקטים ישמש בסיס יציב לתכנון, שאפשר יהיה להוסיף לו אמצעי הגנה, בקלות יחסית.

ארגונים צריכים להבטיח שימוש בכללי ניהול כח-אדם, שהוכיחו את עצמם לאורך השנים. כללים אלה, שהוצגו בפרק 5, כוללים הפרדת תפקידים, רוטציה בתפקידים והגבלת הכניסה; נוהלים לגיוס עובדים והפסקת עבודה ופיקוח על כל עבודה (FIPS 73, 1980). אופן השימוש בכללים אלה תלוי לא רק במערכת המידע, אלא אף במאפייני הארגון. לדוגמה, ארגון קטן עשוי להגיע למסקנה שאי אפשר ליישם את כל הנוהלים בגלל בעיות של עלות.

6.3 שיטות תכנון

במובנים רבים, בחירת אמצעי אבטחה היא אמנות המבוססת על ניסיון. לכן, יש לשתף בתהליך אנשים מנוסים, בעלי התכונות הבאות:

(1) מסוגלים לראות את היישום בצורה כוללת ומקיפה - להלן, גישת המערכות (צ'קלנד, 1981), בפרק 8.
(2) מכירים שיטות אבטחה נפוצות.
(3) מכירים את מערכת המידע הנדונה ואת הפגיעויות שלה.

סעיף 3 לעיל מחייב את אנשי הארגון. רשימות תיוג תורמות לסעיפים 1 ו-2 לעיל. שיטות אחרות, העשויות לסייע לסעיפים 1

ו-2 ידונו בסעיפים הבאים, בכללן, מתודולוגיה לבחירה מסודרת של אמצעי הגנה. טבלה 6.2 מציגה מתודולגייה שמבוססת על הנחיות מכון התקנים האמריקאי (NBS), כפי שתוארו בתקן FIPS 73 (1980), והיא מתאימה ליישומים חדשים ולאחזקה של מערכות קיימות.

לא נתייחס למערכת ההפעלה, שבשליטתה פועלת התוכנה היישומית החדשה, מכיוון שהגבול בין התוכנה היישומית למערכת ההפעלה משתנה מאוד בין מערכות הפעלה שונות. ההנחה היא שברוב המצבים מערכת ההפעלה מספקת אמצעי אבטחה ראויים, כמו ניטור ורישום, כדי ליצור סביבה שבה יוכל מתכנן מערכת המידע לעבוד בבטחון. המתכנן אחראי לכך ששילוב כל הבקרות יעמוד בדרישות האבטחה.

טבלה 6.2 קווים כלליים של מתודולוגיה לשילוב מאפייני אבטחה בממשק של התוכנה היישומית ובתוכה

שלב הפרוייקט	שלבים בתכנון של מאפייני האבטחה
(1) חקר ישימות וניתוח	1.1 נתח את **הפגיעויות** של היישום ונתוניו. 1.2 ציין את **דרישות האבטחה** כחלק אינטגראלי של דרישות המשתמש.
(2) תיכנון מפורט של המערכת	2.1 תכנן **מישקים**, כדי למנוע סיכונים ספציפיים. 2.2 תכנן **בקרות בסיסיות**, כדי לנהל סיכונים בלתי נמנעים. 2.3 סיים את שלב התכנון **בסקירה מובנית** של אמצעי האבטחה.
(3) בניית התוכנה	3.1 בקר את התכנון למניעת השפעות של **שגיאות ומלכודות** מכוונות. 3.2 בדוק את תגובת המערכת לקלט **לא רגיל או מזויף**, ואת התנהגותה בנסיבות מיוחדות.
(4) לאחר ההתקנה	4.1 בדוק שממלאים אחר נוהלי האבטחה בעבודה הפקידותית ובעבודות ידניות אחרות. 4.2 שלב מאפיינים נוספים בתוכנית לשעת חירום.

6.3.1 מתודולוגיה לפיתוח אמצעי אבטחה בתוכניות יישום

הקווים הכלליים של המתודולגייה הוגדרו בטבלה 6.2. חלק מההצעות נראות כהליכי תכנון רגילים של מנתחי מערכות, ולכן נתייחס רק להיבטים הקשורים באופן מובהק באבטחה. את מקורן של בעיות רבות בתוכנה אפשר למצוא בחקר הישימות, שאינו מכיל מספיק הגדרות שקשורות למטרות האבטחה. המשתמשים צריכים להגדיר את ההחלטות הקשורות באבטחה כיעדים כלליים ולהשאיר בידי המתכננים את בחירת הדרכים הטכניות להשגת יעדים אלה. לעתים קרובות, אפשר ליישם בקרת אבטחה מסוימת בעזרת נוהלים, או בעזרת בקרות בתוכנה. עדיף להשתמש בבקרות אוטומטיות, שעלות התפעול שלהן קטנה יותר והן עקביות יותר מבקרות ידניות. בשלבים המוקדמים של הפיתוח חשוב לזהות איומים ופגיעויות, השונים בכל מערכת. דוגמאות טיפוסיות שלהן מובאות בטבלה 6.3.

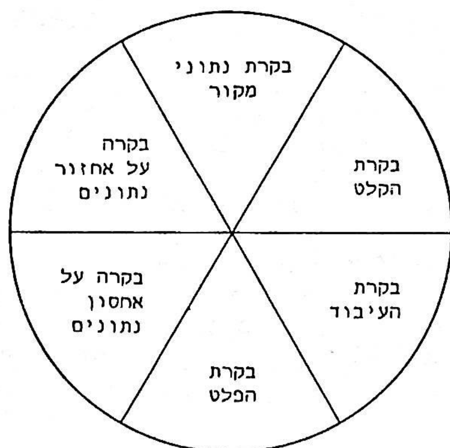
טבלה 6.3 איומים, פגיעויות ובקרות

איומים	פגיעויות	בקרות בסיסיות
1. פעולות מכוונות 1.1 הכנסת נתונים ללא הרשאה 1.2 שינויים בתוכנית 1.3 שינויים בקובץ **2. פעולות בשגגה** 2.1 שגיאות קלט 2.2 שגיאות עיבוד 2.3 קלט שגוי 2.4 הצצה מתוך סקרנות	1. שיטות פיתוח גרועות 2. גישה למשתמשים רבים 3. הדרכה גרועה לאנשים שמזינים נתונים 4. בקרות גרועות על הכנת נתוני המקור 5. בקרות גרועות על שידור הנתונים והפצתם 6. צוות המחשב המקצועי אינו מוצא אתגר בבקרות על הכנסת נתונים	1. תכנון מגן (כלומר, מערכות שפועלות בסביבה עויינת) 2. בקרות שניתנות לבדיקה. 3. הצפנה. 4. אפשרות לזיהוי כל משתמש 5. אחריות על אובייקטים רגישים

שלב התכנון המפורט חייב להגדיר את תחומי האחריות של כל האנשים הקשורים בתוכנה היישומית, באמצעות המישקים השונים. כל פונקציה שעוזרת להתחבר ליישום היא מישק. המישקים נועדו לביצוע מטלות שונות בתוכנית, למשל:

(א) איסוף נתוני מקור.
(ב) הכנסת נתונים.
(ג) חלוקת הפלט.
(ד) תפעול המחשב וניהול ביצוע העבודות.
(ה) ביקורת.
(ו) תחזוקת התוכנית.
(ז) תחזוקת בסיס הנתונים.

יש להשקיע מחשבה בכל מישק, כדי להעריך את הסבירות והתוצאות של שגיאות ופעולות מכוונות, ועל פיהם לקבוע את הבקרות הדרושות. ניתוח כזה מיועד, בדרך כלל, למשתמשים שאינם אנשי מחשב. יש לבצע ניתוח דומה להתנהגות אנשי המחשב המקצועיים. לדוגמה, קיימות תוכניות שירות רבות עוצמה, שיש לאפשר לתוכניתנים ולמנתחי מערכות להשתמש בהן רק תחת פיקוח הדוק של ההנהלה. בעזרת תוכניות שירות אלו אפשר לשנות את המאפיינים הפנימיים של המערכת במהלך פעולתן, מבלי שגורמים אחרים יהיו מודעים לשינויים (סאמוקוויק, 1982). פגיעות זו מאפשרת פעילות סודית בהיקף גדול, וכך יוצרת איום משמעותי. אפשר למצוא בקרות לאיום מסוג זה, ומסוגים אחרים, ברשימות התיוג שהוזכרו בפרקים קודמים.



תרשים 6.2 בקרת נתונים בתוכנה יישומית

בסוף שלב התכנון המפורט, כדאי לערוך סקירה מובנית (structured walkthrough) של תכנון האבטחה על ידי קבוצה שכוללת את המשתמש ואת מומחי המחשב. בדיקת חברים למקצוע יעילה מאוד, מכיוון שהיא מאפשרת למתכנן ייעוץ מקצועי פורמלי, בהשקעה קטנה של זמן (פייג'-ג'ונס, 1980). אפשר להשתמש בתהליך סקירה מובנית בכל שלבי פיתוח המערכת, כמו לדוגמה, ביקורת שלבי התכנות והניסוי.

שגיאות תכנות הן סיבות נפוצות לאובדן וקשה מאוד לגלות אותן לאחר שהוכנסו לתוך הקוד. כדי למנוע מקרים מסוג זה, יש להשתמש בטכניקות הטובות ביותר להנדסת תוכנה ובכללן בדיקה דינמית וסטטית. בדיקה דינמית משתמשת בנתונים שנקבעו מראש להשוואה בין תוצאות הניסוי לתוצאות הצפויות. בדיקה דינמית אפשרית רק לחלקים מתוכניות, ולכן יש להיעזר בנתחי תוכניות לתהליך הניסוי. בעזרת נתח (תוכנית שירות לניתוח - program analyser), האוסף נתונים על התוכנית של היישום במהלך ביצועה, ניתן לקבוע את העובדות הבאות:

* אם נתוני הניסוי גרמו לכל הפקודות בתוכנית להתבצע.
* מידת השימוש בתוכנית.
* קוד לא רגיל, או קוד שאין לו שימוש, שעלול להיות בלתי חוקי.

הניסוי צריך להבטיח שהושג התפקוד הדרוש ושביצועי היישום יהיו מספקים בנסיבות יוצאות דופן.

6.4 בקרות בתוך התוכנה ובמישק של התוכנה

אחת התופעות הקיימות היא של משתמשי מחשב המתלוננים על קבלת מידע שטותי. תקלה זו נובעת בדרך כלל מטעות אנוש, ורק לעתים רחוקות זוהי תקלת מכונה. הנוהלים לעבודות פקידותיות, שהם חלק ממערכות מידע המבוססות על מחשב מועדים לטעויות יותר מתוכנות היישומים. בפרק זה נדון בבקרות בסיסיות, שיש לקבוע בתוכנה היישומית ומסביבה, כדי להקטין את כמות הטעויות ולהשיג יעדי אבטחה נוספים. בתרשים 6.2 אפשר לראות את המקומות שבהן ניתן להתקין את הבקרות, ובטבלה 6.4 ניתן לראות בקרות טיפוסיות שאפשר להתקין בתוך התוכנה היישומית ומסביבה. דיון מפורט יותר בנושא זה ניתן למצוא ב-FIPS 73 (1980) ואצל סקווירס (1980).

טבלה 6.4 אמצעי הגנה טיפוסיים שניתן לשלב במערכת מידע

התהליך	אמצעי הגנה שיש לשקול בזמן תכנון המערכת
1. יצירת נתוני מקור	1.1 תכנון מסמכי מקור 1.2 אחסון מסמכי מקור 1.3 אישור מסמכי מקור
2. הכנת נתונים לקלט	2.1 מסמכי אצווה מאוחסנים קרוב למקור 2.2 גודל האצווה ומספר סידורי 2.3 רישומי בקרה המכילים פרטים על העברת מסמכים
3. הכנסת נתונים (כולל המרה עריכה ואימות)	3.1 המרת הנתונים תתבצע בקרבה פיסית למקום שבו נוצרו הנתונים. 3.2 הגבלת כניסה למסופים ורישום ניסיונות כניסה כושלים למערכת 3.3 אימות נתונים ואצווה
4. עיבוד	4.1 סיכומים לצורך בקרה (control totals) 4.2 בקרת ציפיות (anticipation control) 4.3 רישומים לצורך בקרה (control logs)
5. פלט של נתונים	5.1 רישום במחשב 5.2 נוהלים לבדיקת התאמה (לדוגמה, בין מספר המסמכים שעובדו, לבין מספר המופיע בבקרות האצווה)
6. פיזור של הפלט	6.1 רישום של תאריך ושעת המסירה 6.2 בדיקות התאמה (פלט צפוי התקבל, בדיקה צולבת לאבטחת שלימות) 6.3 נוהלים מיוחדים עם רמת רגישות גבוהה
7. אחסון נתונים	7.1 נוהלים לשחזור קבצים
8. טיפול בטעויות	8.1 נוהלים ודוחות, כדי להקל על תיקון שגיאות ועל שידור נתונים מחדש

6.4.1 בקרת נתוני מקור

אחד מיעדי התפעול העיקריים הוא רישום נכון של הנתונים בזמן המתאים. נתונים יכולים להיווצר בצורה הניתנת לקריאה ישירה על ידי מכונה, או בכתיבה מסורתית, שאינה ניתנת לקריאה במכונה. מסמכי מקור, הכתובים ביד בדרך כלל, דורשים, ואף מקבלים, יותר הגנה. לכן, נרכז את הדיון בהמשך במסמכים הכתובים ביד, מכיוון שההגנה עליהם צריכה להיות מספקת גם במקרה מיוחד של נתונים המותאמים לקריאה במכונה. בכל המקרים יש להפעיל בקרות על התחומים הבאים:

* **אמצעים** - טופסי קלט צריכים להיות שמורים באופן בטוח והגישה אליהם צריכה להית מוגבלת לאנשים מורשים בלבד.
* **תכנון הצורה** - תכנון טוב של טפסים יעודד אישור מתאים, יספק נתיב בקרה ויבטיח שהנתונים יהיו מדויקים ושלמים. במקרים רבים, מספר סידורי יספק בסיס לזיהוי ממלא הטופס.
* **מסמכים מיוחדים** - אמצעים מיוחדים דורשים הגנה מיוחדת. למשל, טופס להתאמת רמות מלאי יוחזק על ידי המבקר, או על ידי מנהל בכיר.

בנוסף, יש לקבוע נוהלי בדיקה ואישור, שיושגו בעזרת חתימה על מסמכים, סיסמאות ומספרי זיהוי למסופים. בכל מקום בארגון שנוצרים בו נתוני מקור, תבחר ההנהלה עובדים שיהיו אחראים על מתן אישור לנתונים העומדים בקריטריון מסוים. נתונים שלא יעמדו בקריטריון זה יועברו לסמכות גבוהה יותר.

לאחר שנוצרו נתוני המקור, יש להכין אותם להקלדה, לשם הזנה למחשב. משמעות פעולה זו שהמשתמשים חייבים לבדוק באופן ידני את הנתונים. עבודה זו כוללת בדיקת זיהוי מתאימה למסמכים וציון מספרי זיהוי (לדוגמה, מספר תנועה) לצורך נתיב הביקורת:

* מסמכי אצווה בקבוצות, כדי לאפשר התאמה בשלב מאוחר יותר.
* מתן מספרים לאצווה, לצרכי זיהוי ורישום.
* רישומי בקרה לאצווה של מסמכים במהלך מעבר בין נקודות שונות של רישום, או ביקורת.

לאחר העיבוד, יש לשמור את נתוני המקור באופן שיטתי לזמן מסוים, ולאחר מכן - להשמידם. תקופת השמירה משתנה בהתאם לאופי מערכת המידע. זו כפופה, במקרים מסוימים, לדרישות החוק, בנוסף לתוכנית גיבוי והתאוששות הנהוגות במתקן או בארגון. בדומה, השמדה תלוייה ברגישות של המידע המעורב ויש לקבוע לכך נוהלי אישור, פיקוח ורישום.

6.4.2 בקרת הקלט - אימות ואישור

אימות נתונים הוא נוהל שמאפשר העתקה מושלמת וללא טעויות של הנתונים, באופן הניתן לקריאה במכונה. טעויות שאינן מתגלות בזמן ההעתקה עלולות לגרום לאובדן של שלימות הנתונים ולהשפיע לרעה על החלטות ההנהלה. אישור נתונים הוא תהליך של בדיקת הנתונים, שלאחריו אפשר לקבוע אם הם מדויקים, שלמים, עקביים וסבירים. נתונים לא חוקיים יכולים לגרום לפלט שגוי ולהרוס את אמינות מערכת המידע. להלן, הטכניקות לאימות הנתונים:

* **סיכומי בקרה:** איסוף של תנועות באצוות (batches) וביצוע סיכום של שדות חשובים. הסיכום יוצר קלט נוסף הנשאר באצווה ואפשר להשתמש בו למטרות השוואה.
* **ספרת ביקורת:** יש להוסיף ספרה או ספרות ביקורת לערכים או שדות חשובים (למשל, מספרי זיהוי)..
* **בדיקה חזותית:** הגרסה המוקלדת מושווית עם נתוני המקור. שיטה זו, המועדת לשגיאות וצורכת זמן, מומלצת רק למקרים מיוחדים, כמו בעת הקלדה ישירה של נתונים. יש לתמוך בה בשילוב עם בקרות אחרות.
* **בדיקת הקלדה:** נתוני מקור מוקלדים פעמיים ומתבצעת השוואה בין שתי הגרסאות. כל שגיאה תוקלד ותבדק שוב. פעולה זו יקרה מאוד ויש לנקוט בה במקרים חריגים בלבד.

שיטות קיימות לבדיקת תקיפות נתונים (data validation) ולאיתור טעיות הן: סיכומי ביקורת (לדוגמה, סיכומי אצווה, ספירת רשומות, והשוואת תנועות) ובדיקות לעקביות, סבירות ושלימות. בבדיקת תקיפות נתונים (data validation) הינה בקרה בסיסית ביותר, אבל אין היא יכולה לעמוד בפני עצמה ויש להוסיף לה בקרות אחרות. בדיקת תקיפות חיונית במצבים הבאים:

* במהלך איסוף נתונים ובמהלך ההקלדה, לפני שהתוכנה היישומית משתמשת בנתונים.
* בהמשך, לאחר שנוצרו נתונים חדשים.

המערכות להזנת נתונים ממסופים מאפשרות פעולה מהירה, אך הן דורשות בדיקת תקיפות אוטומטית ברמה גבוהה. יש לתקן נתונים לא חוקיים במהירות האפשרית, אך הדבר עלול לגרום טעויות. כמו במקרה של נתונים שנדחו ונעזבו לזמן רב לפני שתוקנו. כדי להבטיח שנתונים לא יישכחו, מומלץ שכל הנתונים הלא חוקיים יאוחסנו בקובץ ביניים של התוכנה היישומית, ויבוטלו רק לאחר הוראה מפורשת של המשתמש.

6.4.3 בקרה בזמן העיבוד במחשב

קיימים מספר עקרונות בסיסיים שניתנים ליישום, כדי להבטיח שמירה על דיוק הנתונים ושלימותם במהלך העיבוד במחשב. שגיאות יכולות להתרחש, על אף הדיוק של נתוני הקלט ואמינות המכונה. על אף רמת האמינות הגבוהה של המחשבים, מומלץ לשלב ביישום מאפייני גילוי ובקרה. הפגיעויות כוללות שגיאות בתוכנה, מצב פיסי ירוד של אמצעי האחסון המגנטיים וטעויות הנגרמות מהנחות הנוגעות לאופן הביצוע של פונקציות אריתמטיות.

ניתן לשלב בקרות שיתגברו על בעיות אלו. לדוגמה, קבצים לגישה ישירה ייחסמו לעבודה מקוונת בפרקי זמן ללא פעילות, וייתבצע סיכום כולל של נתונים שונים. במהלך העבודה המקוונת, יתבצע סיכום רץ של שדות חשובים בקבצים, או בבסיס הנתונים. מדי פעם תתבצע השוואה בין הסיכום הכולל החדש לבין הסכום הכולל הישן. מנגנוני בקרה נוספים אפשריים: דיווח על אירועים חריגים, כמו בעת עקיפת בקרה בתוכנית, או פגיעה בסדר הצפוי של הזנת נתוני הקלט.

למרות כל הנאמר לעיל, הבקרה הבסיסית היעילה ביותר לשימוש במהלך העיבוד ובזמנים אחרים, היא רישום אוטומטי של אירועים נבחרים. תיאורטית, הרישום צריך להכיל את כל האירועים, אך אין זה אפשרי מבחינה מעשית. הרישום מכיל אירועים נבחרים בלבד, בהתאם ליעדי האבטחה של כל מערכת. יש להחליט על תוכן קובץ האירועים רק לאחר שיתבצע ניתוח מתאים, שמטרתו לזהות את פרטי המידע שיירשם, את התקופה שיש לשמור את הנתונים, את הדוחות שיש להפיק על סמך מידע זה ואת אופן הניתוח של הנתונים הנאגרים. קובץ אירועים טיפוסי יכיל את הפרטים הבאים:

(1) אופי האירוע: כמו קלט או פלט של נתונים, או שימוש במערכת.
(2) זיהוי של המשתמשים והאובייקטים המעורבים: יש להשתמש במספרי זיהוי של משתמשים והתקנים.
(3) מידע המתייחס לאירוע: תאריך ושעה, הצלחה או כישלון ועובדות מתאימות ואחרות, הנוגעות לרשומות שלפני האירוע ואחריו.

יש לזכור שרישום המופק על ידי המערכת היישומית יכיל פעילויות המבוצעות באותו יישום בלבד. יש להשתמש ברישום אירועים באופן מבוקר, שאם לא כן, יקטנו הסיכויים לגילוי פגיעה באבטחה, מכיוון שהמערכת תהיה עסוקה ברישום, התקשורת תהיה עמוסה והמחשב לא יעסוק במשימתו העיקרית - הרצת תוכניות יישום.

6.4.4 בקרת הפלט

משתמש ישפוט מערכת מידע לפי הפלט שהיא מפיקה עבורו. לכן, אין לשחרר פלט מהמחשב לפני ביצוע בדיקות שיבטיחו שהוא מושלם ומדויק. הבדיקות נעשות על ידי היחידה העוסקת בבקרת נתונים, שמפקחת על העבודה לפני ואחרי העיבוד במחשב. שימוש רב נעשה ברישום, כמו למשל, השוואה בין הרישום הנוגע לאצוות הקלט, לבין רישומי המחשב לגבי האצוות שעובדו, או שנדחו. לאחר שאושר הפלט, יש לבצע חלוקה למשתמשים מורשים ולהשמר מפני אובדן והפרעה. יש לקבוע את שיטת החלוקה לאחר דיונים עם המשתמשים. התוצאה תהיה זיהוי של משתמשים מורשים, מסלולי חלוקה ושיטות תעבורה מוסכמות. בקרת נתונים נעשית בעקבות נוהלים מוסכמים אלה וכוללת רישום המכיל את התאריך, את השעה ואת שם המקבל.

לאחר קבלת הפלט, יבצע המקבל בדיקות דומות, אך מפורטות יותר, ויכין רישום של הדוחות שהתקבלו ובמידת הצורך, יצרף הערות שיופנו למחלקה לבקרת הנתונים. המשתמש יתייחס לרשומות מיוחדות כמסמכים בעלי סיווג בטחוני גבוה, כמו למשל, מסמכים אישיים והמחאות כסף. הוא ינהל עבורם רישום מיוחד לשם ביקורת והתאמה.

6.4.5 בקרה על אחסון ואחזור נתונים

יש למנוע חשיפת מידע, הנמצא באמצעי אחסון, לגורמים שאינם מורשים, ויש למנוע שינוי או הרס של המידע במכוון, או בשוגג. הנתונים פגיעים במיוחד, מכיוון שהאחסון והאחזור כוללים פעילות אנושית רבה. הבקרות חיוניות מאוד בסוגי פעילות אלה והן נעשות באמצעות תהליכי מחשב העוסקים בטיפול בקבצים ובאמצעות נוהלים שונים.

הבקרות נמצאות במישק של התוכנה היישומית. התהליכים המטפלים בקבצים הם חלק מתוכנת המערכת והם נשלטים על ידי הבקרות הבאות, שתוארו בפרק 3: הרשאה, בקרת ההיקש הלוגי והצפנה. מתכנן שעומד לתכנן מערכת מידע בטוחה, חייב להעריך את הנקודות החזקות והחלשות של מנגנונים אלה. יש לשמור אמצעים לא מקוונים לאחסון נתונים בסביבה מתאימה, שאפשר להגביל את הכניסה הפיסית אליה. האדם היחיד שצריך לאפשר לו גישה לשטח זה הוא האחראי על אמצעי האחסון, הספרן, שיודע על כל התנועות של אמצעי האחסון. הוא מבצע רישום שכולל את הפרטים הבאים:

(1) הסרט, או הדיסקט שנלקח.
(2) היעד.

(3) חתימת ידו של המושך.
(4) מועד צפוי להחזרה.

ההגנה על אמצעי האחסון המגנטיים דורשת תחזוקה של עותקי גיבוי באתרים אחרים. באחריות ההנהלה לקבוע מהו מידע רגיש וקריטי שמחייב גיבוי. לאחר שנקבעה המדיניות, יש לטפל, כמשימה שגרתית, ביצירת עותקי הגיבוי ובאחסונם במקום המרוחק ממרכז המחשבים. שני הנושאים, בקרה של מידע הנמצא באמצעי אחסון לא מקוונים ותחזוקה של עותקי הגיבוי, יוסברו שוב בפרקים 7 ו-11.

טבלה 6.5 עקרונות אבטחה בסיסיים שניתן להשתמש בהם בתכנון

עיקרון	הסבר
תכנון לא סודי	מערכת חדשה תהיה טובה יותר אם המאפיינים שלה יהיו חשופים לביקורת של עובדים רבים, הן מתכננים והן משתמשים.
מערכת שמקובלת על המשתמשים	על כל מישק בין התוכנה היישומית והמשתמשים להיות פשוט וטבעי למשתמש, שאם לא כן, הוא ייעקף.
התערבות מלאה	יש לבדוק כל גישה, לכל אובייקט, כדי לראות אם המבקש מורשה לכך.
ברירת מחדל למצב שבו נדחית בקשת הגישה	אם קיים ספק בבקשת הגישה, יש לדחות אותה, כי דחייה עדיפה על גישה ללא הרשאה.

6.5 סיכום

בתכנון מערכת מידע, יש להניח שהיא תפעל בסביבה עוינת, תחת איום זה או אחר. בעבר לא הושם דגש על נושאים אלה והיתה נטייה להתעלם מדרישות האבטחה, עד לשלב שבו התחילה המערכת את פעולתה. כדי שמערכת תהיה בטוחה, על התוכנה היישומית למלא אחר העקרונות המופיעים בטבלה 6.5 (הופמן, 1977). אפשר לבצע זאת באופן חלקי, באמצעות המתודולוגיה והבקרות שתוארו בפרק זה, אך אין זה מסריק. יש להוסיף על כך רעיונות רבים ושיטות

אחרות. לדוגמה, להרשאה, לבקרת ההיקש ולהצפנה יש מגבלות שהמתכנן חייב להתחשב בהן במהלך תכנון המערכת. בדומה, השיטה המתוחכמת של ניתוח סיכונים, המוצגת בפרק 8, היא כלי עזר מצויין למתכנן, ויש להשתמש בה להשלמת השיטות שתוארו לעיל. גישה רחבה וכוללת לאבטחה תיצור סביבה שבה הבקרה, המשולבת בפעולות אחרות, תהיה מקיפה. בתכנון האבטחה של התוכנה חובה לבצע את הפעולות הבאות:

(1) לחפש את הגורמים בארגון שיכולים להשפיע על האבטחה.
(2) להגדיר גישה כללית לתכנון אבטחה.
(3) לשלב, בתוך התוכנה ובסביבתה, בקרות שהוכיחו את עצמן לאורך שנים.

מכיוון שאין אלו משימות פשוטות, יש לפתח את מאפייני האבטחה של התוכנה היישומית כמשימה משותפת של המתכננים והמשתמשים של מערכת המידע.

שאלות

6.1 אבטחה דורשת שילוב של חוקים ואמצעי הגנה טכנולוגיים, פיסיים ומנהליים. אם החוקים יהוו שישה אחוזים מכלל הבקרות, כמה אחוזים יהוו כל אחד משאר המרכיבים?

6.2 פרט ותאר ארבע בקרות שונות שאפשר לבנות בתוך תוכניות.

6.3 בדוק מערכת מידע שאתה מכיר ותאר את הפרטים הבאים:
(א) נקודות הביקורת העיקריות שלה.
(ב) מנגנוני בקרה מתוכנתים לקלט, שניתן ליישם אותם בין שלב קליטת הנתונים על ידי המחשב לבין הפיכתם לתנועות קלט תקיפות המיועדות להמשך העיבוד.
(ג) מנגנוני בקרה מתוכנתים ליצירת פלט מחשב.
השווה בין הבקרות שצוינו בתשובותיך הקודמות לבין אלו הנמצאות בתרשים 6.2. פרט ותאר מאפיינים נוספים לאותם חלקים בתרשים שלא הצעת עבורם מנגנוני בקרה.

6.4 האם חשובה הבקרה על תיעוד? הסבר.

פרק 7

ההיבטים באבטחת התפעול של מתקני מחשב

לאחר שהתוכנה היישומית פותחה ועמדה במבחנים מקובלים, היא מהווה חלק ממערכת המידע, שעוברת לשלב התפעול. במהלך שלב זה, יש להמשיך ולהקפיד שרמת האבטחה לא תרד, כדי שהמאמץ שהושקע בבניית הבקרות שבתוך התוכנה היישומית לא יירד לטמיון. לעבודה של אגף התפעול חשיבות עליונה ועליה להיות אמינה. אפשר להשתמש בכמה נוהלים לצורך השלמת הבקרות הנמצאות בתוך התוכנה היישומית ובסביבתה (IBM, 1976). להלן, ההיבטים התפעוליים המשפיעים על האבטחה:

* מדיניות החברה בנושא הכניסה למתקני המחשוב.
* המחויבות והמעורבות של צוות התפעול.
* תוכנית להתאוששות.
* תחזוקת התוכנה והחומרה.

היבטים רבים אחרים של האבטחה מסייעים לתפעול בטוח, כמו למשל, אבטחת נתונים, אבטחה פיסית ותוכנית לשעת חירום. נושאים אלה מתוארים גם בפרקים אחרים בספר זה והחפיפה ביניהם בלתי נמנעת, אך נציג אותם להלן מזווית התפעול.

7.1 אבטחת התפעול והשימוש ברישומים

אבטחת התפעול קשורה באופן בסיסי למדיניות החברה ולנוהלי אבטחת הנתונים ומתקני המחשב. חלק קטן מקווי המדיניות והנוהלים נועדו לענות על דרישות חיצוניות, כמו חוקי הגנת הפרטיות למשל, אך רובם נקבעים על ידי ההנהלה. קווי מדיניות אלה נחלקים לשני הסוגים הבאים:

(1) אמצעי הגנה, שנקבעו במהלך הפיתוח ונבנו בתוך התוכנה היישומית ובסביבתה (רבים מהם תוארו בפרקים הקודמים).
(2) אמצעים הקשורים בארגון ובביצוע של פעולות התפעול.

קיימות כמה שיטות שקשורות לסוג השני, ביניהן בקרה על נתונים במהלך הכנת נתוני קלט (ראה פרק 6); כללי ניהול כח-אדם (ראה פרק 5); תגובה לאירועים חריגים הקשורים באבטחה (FIPS 73,

1980) שנדונה בפרקים 5 ו-8. שיטה נוספת, שמוסברת בפרק 6, היא רישום אירועים.

7.1.1 רישום פרטי ההפעלה

רישום פרטי ההפעלה (operating journals) מכיל את הנתונים הבאים:

* פרטי הריצה של תוכניות.
* הקבצים שהשתמשו בהם.
* המסרים שבין התוכניות לבין מפעיל המחשב.
* תקלות במהלך הריצה.

קשה לבדוק את הדפסי הריצות המופקים על ידי המחשב, אך למרות זאת, יש לבחון אותם היטב ולשמור אותם לצרכים עתידיים, כמו ביקורת.

לאירועים מסוימים חשיבות רבה ויש לרשום אותם בנפרד. לאירועים הבאים יש להקדיש תשומת לב מיוחדת:

* תקלות בציוד.
* חידוש ריצת תוכנית מנקודות ביקורת, (checklist, נושא שמוסבר בסעיף 7.5.1).
* תקלות בתוכניות במהלך הריצה.
* אישוש, או שיחזור, של קבצים.
* יצירה מחדש של קבצים.

7.2 גישות לתפעול מתקני מחשב

אפשר למנוע שימוש ללא הרשאה במשאבי המחשב באמצעות בקרות והגבלות שיוטלו על ידי ההנהלה. אחת ההחלטות החשובות ביותר בענין זה קשורה לכמות האנשים שצריכים לגשת למתקני המחשב. הכניסה מבוקרת על ידי הסביבה התפעולית, בשלושה סוגים עיקריים:

(1) **הפעלה סגורה:** האנשים היחידים שרשאים לגשת למחשב הם מפעילי המחשב, שמקבלים את העבודות לביצוע ומפקחים על תהליך העיבוד.
(2) **הפעלה פתוחה:** כל אחד מהעובדים רשאי לגשת למחשב ולהריץ עבודות כלשהן.
(3) **כניסה לא מוגבלת דרך קווי תקשורת:** המשתמש לא צריך לבקר במרכז המחשבים, או ליצור קשר עם מפעילי המחשב.

קיימות גרסאות רבות לסביבות עבודה אלו (האיסו, 1979), אך סוג הסביבה שבו ישתמש הארגון חייב להיות מתואם לאופי הארגון. סביבה סגורה מתאימה למתקן צבאי בעל דרישות אבטחה גבוהות. בסביבה זו גורמים מנגנוני האבטחה אי-נוחות למשתמשים. כללית, סביבת התפעול חייבת להיות נוחה למשתמש, במיוחד כאשר יישומים מודרניים רבים עובדים במקוון, כלומר, בסביבה של גישה לא מוגבלת. סביבה זו אידיאלית למשתמש, אך יש בה מגרעות כי היא חשופה מאד לפעולות לא חוקיות שעלולות להתבצע על ידי משתמשים מורשים. סביבה חייבת להרתיע עבריינים פוטנציאליים ולמנוע, או לגלות, פגיעות במערכת.

7.3 צוות התפעול

מערכת מתוכננת היטב תרוץ במחשב ללא עזרת המפעילים, או בעזרה מעטה מצידם. הפעולות שעל המפעיל לבצע צריכות להיות פשוטות יחסית ורצוי שאי אפשר יהיה ללמוד בעזרתן על המערכת, או על המידע המעובד. במקרה של הכנסת נתונים ישירה, או הזנת עבודות מרחוק ממסופים, אין המפעיל רואה דבר הקשור לקלט, פרט להודעות בקונסול. גם אם העבודה תוגש דרך המחלקה העוסקת בבקרת הנתונים, על המערכת לפעול באופן דומה. המחשב צריך לבקר את הפעולות ולתת מידע מינימלי למפעילים. על מצבים ותנאים יוצאי דופן, או על חריגים בתהליך העיבוד יש לדווח בפלט של המשתמש.

מספר קטן ככל האפשר של אנשים צריך לטפל בפלט, כדי למנוע מרבים להציץ בו. על הפלט לעבור, מיד לאחר העיבוד, למחלקת בקרת הנתונים, לשם מיון, בדיקה ופעולות אחרות (כמו, הכנה לדפוס או ארגון החומר בסדר כלשהו רצוי להפצה). יש לדאוג לסימון הפלט על ידי המחשב, כדי לעזור למיון וכדי להקטין, ככל האפשר, את הסכנה שהנתונים יגיעו בטעות למי שלא צריך לקבלם.

עבודה הנשלחת דרך מחלקת בקרת הנתונים פגיעה יותר מעבודה שנשלחת מרחוק, דרך מסופים, מכיוון שהיא עוברת דרך מחלקות רבות ושונות, ומכיוון שבקרות הכניסה, המשמשות לזיהוי והרשאה של משתמשי מסוף, אינן פועלות כאן. למרות כל זאת, ניתן ליצור סביבת תפעול מוגנת בעזרת התערבות מינימלית של מפעילים, משתמשים, בקרי נתונים וספרני קבצים.

7.3.1 הדרכת מפעילי מחשב

אין לצפות ממפעילי מחשב ומעובדים אחרים להתנהג באופן שתואר

לעיל ולפעול באחריות בנושאי אבטחה, אם לא הודרכו וקיבלו עידוד לכך. חיוני להעביר למפעלי המחשב ידע כללי על מערכת ההפעלה, בקרת המערכת, ציוד בטיחות ואבטחה ותיעוד. יש לידעם באופן מיוחד על המטלות התפעוליות השגרתיות, על משימות האבטחה ולעורר מודעות לאבטחה. בהדרכת משימות האבטחה יש להביא לידיעת המפעילים דברים שעליהם להמנע מלעשות, כמו גם המשימות שעליהם לבצע. המפעילים חייבים להכיר את הפעולות החיוביות שמוטלות עליהם במקרה של אש ופריצה. לדוגמה, על המפעיל לדעת אם, במקרה של חדירת אנשים בטעות לשטח סגור, עליו לגרש את המתפרץ, או להזעיק עזרה באמצעות לחצן האזעקה. ארגונים שיזמו תוכניות הדרכה זכו לתגובות חיוביות מצד העובדים. תוכנית כזו משפרת את המורל וגורמת למפעילים לחוש שעבודתם חשובה לארגון.

7.4 מערכת לניהול הספריה

הרציפות והיעילות של פעולות המחשב תלויות במערכת ניהול ספריה אשר משתמשת בנוהלי בקרה ובסטנדרטים טובים כדי להבטיח שספריות התוכנית וקבצי הנתונים יישמרו בבטחון. בפיתוח מערכת ספריה בטוחה, יש לקחת בחשבון את הגורמים הבאים:

* אחסון של המצעים (media) המגנטיים והגנתם.
* גישה לאמצעי האחסון המגנטיים.
* הגירה של תוכניות מסביבת הניסוי לסביבת הייצור.
* שינויי חירום.
* מדיניות ההנהלה וצרכי הדיווח שלה.

השיטות לאחסון והגנה של המצעים המגנטיים מבוססות על זיהוי אמצעי האחסון הדורשים הגנה ועל היכרות עם עובדים הרשאים לגשת לאותם אמצעי אחסון מוגנים. יש להבדיל בבירור בין סביבת ניסוי שבה כותבים ובודקים את התוכנית, לבין סביבת ייצור שבה התוכנית מעבדת נתונים "חיים". דרישות האבטחה מחייבות שבטרם תהגר תוכנית לסביבת הייצור, היא תעמוד בבדיקות של דרישות התכנון ותפעל באופן צפוי.

כאשר התוכנית נמצאת בסביבת ייצור, על מערכת הספריה להגן עליה בפני שינויים לא מורשים. מערכת הספריה פועלת לפי מדיניות ההנהלה, המצביעה על הצעדים שיש לנקוט במקרה של גישה ללא הרשאה לספריה, או לאמצעי האחסון המגנטיים. ההנהלה צריכה לקבל בקביעות דוחות על פעילות מערכת הספריה, על פרטים של כניסות ללא הרשאה לספריה ועל שינויי חירום בתוכניות. שינויים כאלה נגרמים כתוצאה מאירועים בלתי צפויים, כמו טעות בתוכנית המתגלית במהלך הריצה. מגבלות זמן אינן מאפשרות

לעיתים ששינויי החירום יעברו דרך הנוהלים הרגילים של אישור השינוי, בדיקה והעברה לסביבת הייצור.

כל שינוי חירום יוצר פגיעות, ולאחר שבוצע, יש להקדיש לו תשומת לב מיוחדת, כדי להבטיח שמערכת הספריה לא תפגע. על ההנהלה לבדוק מקרוב את שינויי החירום, לא רק בגלל פגיעות הנגרמות על ידם, אלא גם מפני שקיים סיכוי גבוה ששינויים אלה מצביעים על בעיות בסיסיות, כמו נוהלי בדיקה לקויים. מידע נוסף על מערכות ניהול ספריה ניתן למצוא אצל גילהולי (1980). יש לתכנן את מערכת הספריה באופן שיאפשר לה לפעול נגד אובדן חלקי או מלא של ספריות (של תוכניות וקבצי נתונים) במהלך הפעלת אמצעי נגד הקשורים לנוהלי התאוששות וגיבוי.

7.5 התאוששות בטווח קצר

יש הסבורים שאפשר לבנות מערכת מידע ממוכנת המבוססת על מחשב, שבה אמינות התוכנה היישומית מבטלת את חשיבות נוהלי התאוששות. תפישה זו אופטימית מדי ואפילו מטופשת, גם אם מדובר בתוכנה הטובה ביותר ובחומרה האמינה ביותר. יש לנקוט בגישת תכנון זהירה יותר, המתבססת על התפישה שמערכת המידע תפעל בסביבה עוינת. היתרון בשיטה זו הוא עידודו של המתכנן לצפות את המגוון הגדול ביותר של אירועים שליליים ולנקוט נגדם אמצעי הגנה. גישה זו, שנקראת "ניהול לפי סיכונים", מוסברת בפירוט בפרק 8.

יחידות מחשב מתמודדות עם תקלות קטנות באופן יומיומי. לדוגמה, כאשר יש לחדש עבודה שנעצרה. מצב כזה יתוקן בתוך דקות או שעות. אירועים מסוג, המתוארים בטבלה 7.1, גורמים לעיכוב בעיבוד הנתונים ומוציאים את שירותי המחשוב באופן זמני מכלל פעולה. הם דורשים תוכנית להתאוששות בזמן קצר, שאינה יעילה במקרים המצוינים בטבלה 7.2, שבה מפורטים אסונות שהורסים חלק גדול מהמתקנים. אסונות מסוג זה דורשים תוכנית התאוששות לזמן ארוך, המוסברת בפרקים 8 ו-11. פגיעויות שמבטאות את הצורך בתוכניות התאוששות לזמן קצר ולזמן ארוך מתוארות בטבלה 7.3.

בתגובה לתקלה חייבים להיות במערכת המידע נוהלי התאוששות, שיבטיחו שלתת-המערכת המבוססת על המחשב יהיו המאפיינים הבאים:

* זמן ההתאוששות הממוצע יהיה קצר ככל האפשר.
* גם אם מתרחשת תקלה, יתאפשר המשך פעילות ברמת שירות נמוכה יותר. מצב זה נקרא הדרדרות מתונה (graceful degredation) (ווטסון, 1984).
* התקלה לא צריכה לאיים על האבטחה.
* יכולת להתאושש מכל אירוע.

ניתן להשתמש בכמה מנגנונים ואסטרטגיות לביצוע התאוששות בטווח קצר, כמו גיבוי קבצים, התחלה מחדש בנקודות ביקורת ואמצעים לשחזור קבצים.

טבלה 7.1 איומים שמעכבים את העיבוד ומחייבים תוכנית להתאוששות מיידית

(1) תקלה בחומרה, כמו יחידת דיסק, או התקן אחסון אחר.
(2) טעות של מפעיל המחשב.
(3) טעות בתוכנה היישומית.
(4) שריפה חלקית, כמו שריפת ספריית הסרטים, אך לא הרס כללי.

טבלה 7.2 איומים שיכולים להרוס יחידת מחשב ומחייבים תוכנית התאוששות לטווח ארוך

(1) אש
(2) אסון טבע, כמו הצפה
(3) חבלה
(4) השבתה

טבלה 7.3 פגיעויות שמדגישות את הצורך בתוכנית התאוששות

(1) תלות הארגון במערכת המידע ובעיבודי המחשב. לדוגמה, ארגון שאין לו גיבוי ידני, כמו בנק.
(2) העיבוד חייב להתבצע במועד קבוע או מיידי, כמו במערכת להזמנת מקומות בבתי מלון, או בחברות תעופה.
(3) ריכוז של אמצעי המחשוב.

7.5.1 היכולת להתחיל מחדש (שיתחול)

תוכנית יכולה להפסיק את מהלך הריצה עקב תקלה במערכת ההפעלה, או בתוכנה היישומית ובגלל טעות בנתונים. הניסיון הוכיח שלתוכניות שרצות כ-30 דקות או יותר, נחוץ אמצעי להתחלה מחדש, או אמצעי שיתחול (restart). בדרך זו משתחלים את העיבוד מנקודת ביקורת בתוך התוכנית, ללא צורך בהרצתה. במערכות קטנות, נקודת הביקורת נמצאת למעשה לאחר כל עדכון של קובץ ראשי, על ידי העתקה לשם גיבוי.

במערכות גדולות, שמעבדות קבצים גדולים ורבים, כמו בחברות חשמל וגז המנהלות חשבונות של לקוחות ושירותים, ובמערכות פיננסיות, כמו בנקים, ובמוסדות וארגונים ציבוריים, דרושים אמצעים מיוחדים להתאוששות. האמצעי הראשון הוא הכנת העתק של מצב התוכנית בפרקי זמן קבועים. בשיטה זו מתבצע בנקודת העיבוד צילום של כל תמונת העיבוד, הכולל את הזיכרון ומידע על הציוד ההיקפי. המידע מאוחסן על קובץ וניתן לאחזר אותו באופן שיאפשר לשחזר את מצב התוכנית לזה שהיה בנקודת הביקורת.

אמצעי זה אינו משחזר את הקבצים בנקודות הביקורת שלהם ולכן נדרש אמצעי נוסף שיעשה זאת. הנוהל הוא לשמור את כל שינויי הרשומות שבוצעו מאז שנעשה ההעתק האחרון של הקובץ, כדי שאפשר יהיה להשתמש בהם לשחזור הקובץ באמצעות תוכנית שרות.התוכנית לשחזור הקבצים משתמשת גם בנתונים שנשמרו בנקודת הביקורת. יש שתי דרכים לבצע את השחזור:

(1) **לאחר מעשה:** עותקים של הרשומות נלקחים לאחר העדכון, כדי שניתן יהיה לשחזר גרסה מוקדמת של הקובץ, עד לנקודת הביקורת.

(2) **לפני מעשה:** עותקים של הרשומות נלקחים לפני העדכון, כדי שניתן יהיה להשתמש בגרסה מאוחרת של הקובץ, לשם איתור המקום שעד אליו בוצע העדכון לפי נתוני נקודת הביקורת.

מאפיין נקודת הביקורת והאמצעים לשחזור קובץ הם חלק מתוכנת המערכת וקשורים זה בזה באופן שמאפשר התאמה מושלמת בין כל הקבצים במערכת.

7.6 תחזוקה של תוכנה וחומרה

שינויים בתוכנה ותחזוקת החומרה הן פעולות חיוניות בתהליך ההתפתחות של כל מערכת. למרבה הצער, שתי הפעולות הללו עלולות

ליצור איומים. שגיאות עלולות לחדור למערכת במהלך שינוי תוכנית ולהשפיע על שלימות הנתונים. יש סיכון שאף יוכנס במכוון קוד לביצוע פעולה לא חוקית. בזמן תחזוקת החומרה יכולים להתגלות נתונים סודיים לצוות התחזוקה.

יש לבקר את הכנסת השינויים בתוכנה, באופן שבו מבקרים תכנות ראשון (וורינג, 1978). בסעיף 8.5 הוסבר שפרק הזמן שבו מתרחש השינוי בתוכנה הוא מצב זמני שדורש תשומת לב מיוחדת. ההגנות אפשרויות נוספות מפני שינויים בתוכנה יכולות להיות: בדיקת השינויים על ידי ההנהלה באופן שוטף ויסודי, רישום מפורט של כל השינויים, תקנים ונוהלים לאישור, תכנות וניפוי של התיקון.

תחזוקה מונעת ושוטפת היא תהליך חיוני במערכת. אם נמצא ברישומים שהמערכת נופלת לעתים קרובות, יש לבדוק את תדירות התחזוקה. במהלך התחזוקה אין להשתמש בנתוני הייצור, אלא בנתוני ניסוי בלבד. יש להפעיל מעקבים (traces) למהלך התוכנית והנתונים.

7.7 סיכום

תפעול המחשב הוא פעולה חשובה וקריטית לארגון והראינו אופנים שונים לעשותה מאובטחת יותר. עבריין פוטנציאלי צריך לדעת כיצד לגשת למערכת המידע ולהכיר את צורת התפעול שלה. לכן, נוהלי תפעול בטוחים תלויים באכיפה של כללים שהוכחו כיעילים לאורך השנים, כמו הפרדת תפקידים ועיקרון "הצורך לדעת". יש לבצע גם את נוהלי האבטחה שנבנו בתוך המערכת ולא להתעלם מהם. האחריות היא בידי ההנהלה, שצריכה להדגיש בפני העובדים את החשיבות של האבטחה בזמן הפעילות השגרתית של המערכת. אם לא ייעשה כך, כל המאמץ שיושקע בתכנון האבטחה יהיה לשוא.

שאלות

7.1 הסבר את אופן השימוש של בקרת אצווה במערכת מקוונת. מהם חסרונות שיטה זו ואילו נוהלים ישיגו בקרה דומה ביישום מקוון?

7.2 תוכנית שרושמת את כל פרטי התנועות שבוצעו על ידי משתמשים בבסיס נתונים מגדילה את תקורת המערכת. האם יש בכך חסרונות אחרים?

7.3 הסבר את המושג "ניטור איומים".

פרק 8

פיתוח והערכה של תוכנית אבטחה לארגון

בפרק זה מוסברות טכניקות לניתוח סיכונים (שגם מזהות צרכים) שיהוו, מאוחר יותר, בסיס ליישום אמצעי האבטחה. לאחר מכן, נדון בשיטות כמותיות לניתוח סיכונים ובקשיים ליישומן. נציג גם כמה שיטות איכותיות.

נציג מתודולוגיה להערכה או לפיתוח של תוכנית אבטחה, שתופנה בעיקר לשאלת האבטחה מנקודת מבט של תורת הכרת המערכות, שהרי המערכת שאת האבטחה שלה אנו בודקים, נמצאת בתוך מערכת גדולה יותר. מתודולגיה זו משתמשת בשיטות כמותיות ואיכותיות.

למרבה הצער, אמצעי אבטחה אינם יכולים לספק הגנה בכל הנסיבות, ולכן נדרשות תוכניות לשעת חירום למקרה של פגיעה במערכת.

יש לזכור את החשיבותם של האנשים המשתלבים בשיטות שתוארו ובסביבתן. לדוגמה, השיפוט המקצועי של המרכיב האנושי הוא הבסיס לזיהוי ולבחירה של אמצעי ההגנה ולמעשה, כל אמצעי ההגנה תלויים, במידה זו או אחרת, בתפקוד של אנשים. אנשים הם מרכיב בסיסי בכל מערכות האבטחה ולעתים קרובות, הם גם המרכיב החלש ביותר.

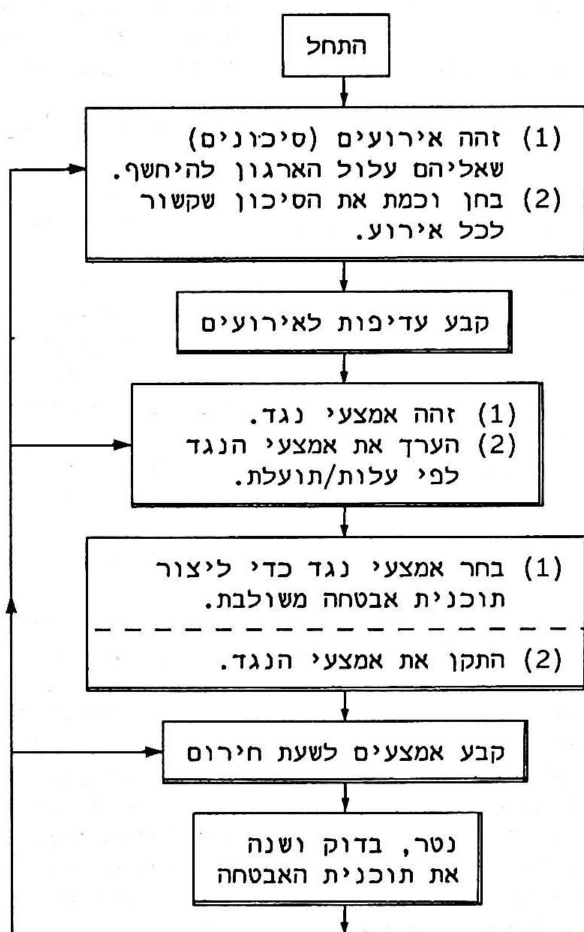
8.1 ניהול לפי סיכונים

העומד לפתח תוכנית אבטחה לארגון צריך להציב לעצמו את שלושת היעדים הבאים:

(1) זיהוי סיכונים,
(2) ניתוח סיכונים,
(3) בקרת סיכונים.

יעדים אלה נקראים במשותף "ניהול לפי סיכונים" (Risk Management). לצורך זיהוי הסיכונים הפוטנציאליים שמאיימים על הארגון, יש לבצע בדיקה מקיפה של כל המחלקות והעבודות. ניתוח סיכונים, הנקרא לעתים גם "הערכת סיכונים", מטפל בבעיה

המהותית שבסיכון פוטנציאלי, כדי לקבוע את הסבירות להתרחשותו ואת גודל האובדן הצפוי. היעד השלישי של ניהול לפי סיכונים הוא בקרת הסיכון, שבה יש צורך לקבל החלטה המבוססת על מידע שנלקח מניתוח הסיכונים. התוצאות המתקבלות מניתוח הסיכונים נשקלות זו כנגד זו, לשם בחירת דרך הפעולה המתאימה ביותר כנגד כל סיכון. התוצאה הסופית עשויה להוביל לנוהלים חדשים, לרכישת ציוד חדש, או לתוספת של כח-אדם.



תרשים 8.1 ניהול לפי סיכונים - פיתוח תוכנית אבטחה לארגון

כאשר יש לבדוק תוכנית אבטחה לארגון, מותר להניח שהארגון השלים כבר את שלושת שלבי הניהול לפי סיכונים. לכן, מטרת הבדיקה היא למדוד את היעילות של הניתוח הקודם.

להלן קווים מנחים לבניית נוהל לפיתוח ולישום של מדיניות אבטחה לארגון:

(1) ניתוח סיכונים, כדי לספק בסיס לפיתוח מדיניות אבטחה.
(2) בחירת אמצעי הגנה, לפי עיקרון עלות/תועלת, כדי להקטין את החשיפה, או האובדן הצפויים.
(3) התקנת אמצעי ההגנה המתאימים.
(4) פיתוח תוכניות לשעת חירום, שיכילו את הפרטים הבאים:
 (א) נוהלי גיבוי,
 (ב) התאוששות מאסונות,
 (ג) מצבי חירום.
(5) הדרכת העובדים.
(6) תכנון וביצוע של ביקורות אבטחה.
(7) כיוון אמצעי ההגנה והתוכניות לשעת חירום.

הנוהל המתואר בתרשים 8.1 מספק אמצעי זיהוי ופיזור של מנגנוני ההגנה המתאימים. הצלחה או כישלון של אמצעים אלה תלויים, בדרך כלל, בעמדת העובדים. לכן, יש לקבוע את אמצעי ההגנה שבאחריות כל מחלקה או יחידה בארגון. תוכנית האבטחה הכוללת של מערכות המידע נמצאת באחריותן של יחידות ארגוניות רבות (31, FIPS, 1974), כפי שמוצג בטבלה 8.1.

8.2 זיהוי סיכונים - באחריות ההנהלה

לכל ארגון אסטרטגיית אבטחה משלו, שיכולה לצמוח בתגובה לקשיים שהתגלו. אבטחה שהתפתחה בנסיבות כאלו עשויה להיות מספקת, אך סביר להניח שהיא תהיה פגיעה מאוד. נוהל הפיתוח האידיאלי מוביל לכך שתכנון, הכוונה והזנה של תוכנית אבטחה יבוצעו על ידי הנהלת הארגון. גם כאשר פותחה תוכנית האבטחה בנוהל הרצוי, קשה עדיין להחליט על הפעלתה, מכיוון שעל ההנהלה לבחור אמצעי אבטחה שיעמדו בקריטריון של עלות מול תועלת. אמצעי אבטחה מתוחכמים מאוד עלולים להיות מעמסה כספית וניהולית, אך מחסור באמצעי הגנה מתאימים עלול להיות יקר באותה מידה ואפילו יותר, אם ניסיון התקפה כמו מרמה, יצליח. לשם החלטה, על ההנהלה להיות מודעת לפרטים הבאים:

(1) מהו סיכון.
(2) האובדן הכספי במקרה שהסיכון יהפוך לפגיעה באבטחה.
(3) אמצעי ההגנה שעשויים להקטין את הסיכון.

(4) עלותם של אמצעי ההגנה.
(5) ההפחתה הצפויה בסיכון, אם יותקנו אמצעי הגנה מסוימים.

ניתוח הסיכונים (קורטניי, 1977; גלייסמן, 1977; ריד, 1977) נמצא במרכז גישה זו, שמנסה לכמת את הסיכון הקשור בכל אירוע שבמהלכו, או בסופו, ייגרם אובדן. היעד הוא להנפיק להנהלה מידע מספק לקבלת החלטות פיננסיות בנוגע לאמצעי האבטחה. מטרת ניתוח הסיכונים היא הכנת הצהרה כמותית של הבעיות, או האיומים הצפויים, שמערכת המידע של הארגון חשופה להם.

טבלה 8.1 האחריות לאבטחה

הרמה בארגון	מהות האחריות	דוגמאות
הנהלה בכירה	סביבה ארגונית מבוקרת	- ייזום ואישור תוכנית לשעת חירום. - לפעול בכל המקרים שבהם ידעו על הפרת מדיניות האבטחה של הארגון (כמו תנועות לא חוקיות, או לא מוסריות).
הנהלת משתמשים	שלימות הנתונים	- לקבוע נוהלים (לדוגמה, הפרדת תפקידים, או נוהלי אישור). - לאמן ולפתח יכולת של עובדים שניתן לסמוך עליהם ולתת להם הגדרות ברורות לסמכות ולאחריות.
	סודיות ושלימות הנתונים	- לקבוע בקרות פיסיות ובקרות גישה לנכסים ולנתונים. - לקבוע ולתחזק נקודות ביקורת ונקודות איזון. - לפקח שהעבודה תתבצע בהתאם לנוהלים, דרך ביקורות מתוכננות ולא מתוכננות
מנהל יחידת המחשב	סודיות, שלימות ושירותי המחשב	- להבטיח שהחומרה, התוכנה ותפעול המחשב עומדים בדרישות האבטחה
מחלקת כח-אדם	סביבה ארגונית מבוקרת.	- לקבוע תנאי העסקה ונוהלי ראיון עקביים, שיחזיקו במטרות האבטחה של המחלקה והארגון.

8.3 ניתוח סיכונים

נוהל לניהול לפי סיכונים, אשר מכיל ניתוח סיכונים (risk analysis) ומשתמש בו, מתואר בתרשים 8.1. הנוהל עוסק בנושאים הבאים:

(1) זיהוי, בדיקה והערכה של סיכונים בתוך הארגון.
(2) שימוש באמצעי נגד, כדי להקטין את האובדן לרמה שניתנת לספיגה.

ארבע גישות לטיפול בסיכונים:

(1) **למנוע את הסיכון:** משנים את המערכת כך, שיסולק מתוכה מאפיין שמהווה סיכון.
(2) **להקטין את הסיכון:** שימוש באמצעי הגנה להקטנת הסיכון לרמה סבירה.
(3) **להשאיר את הסיכון כמות שהוא:** להתעלם מן הסיכון, אם הוא קטן וחסר משמעות.
(4) **העברת הסיכון:** אין משנים את המערכת, אך הסיכון לאובדן מועבר לארגון אחר. לדוגמה, באמצעות פוליסת ביטוח או הסכם כלשהו.

אחת הגישות המתימטיות לניתוח סיכונים במצב מסוים משתמשת בנתונים סטטיסטיים (וונג, 1977). לרוע המזל, רק לעתים רחוקות ניתן למצוא את כל הנתונים הדרושים לכך. ניתוח סיכונים מוגדר כמנגנון המספק מידע, שמאפשר להנהלה לקבל החלטות הנוגעות לסיכונים, או לצירופי סיכונים. ניתוח סיכונים הוא הבסיס לבחירת אמצעי הגנה, תוך נקיטת גישה שיטתית שכוללת את הפעולות הבאות:

(1) סיווג איומים לנתונים.
(2) סיווג אמצעי הגנה לאיומים אלה.
(3) החלטה על דרך הפעולה שתכוון משאבים טכניים ולא טכניים, לסיכונים בעלי הסבירות הגבוהה ביותר ולסיכונים היקרים ביותר (הופמן, 1977).

קיימות כמה מתודולוגיות לניתוח סיכונים, ביניהן: גישת אילינוי לטיפול כלכלי באבטחה (IBM, 1974), גישת קורטניי (קורטניי, 1977) וגישה המבוססת על תיאורית הקבוצה הנסתרת (הופמן ואחרים, 1978).

לפי גישת אילינוי, ההוצאה המתחייבת משנת שימוש אחת במערכת אבטחה (k), מוגדרת לפי הנוסחה:

C(k) + L(k)

כאשר C(k) הוא ההוצאה (בשקלים לשנה) להתקנה ולתפעול של המערכת (k), ו-L(k) הוא האובדן (בשקלים לשנה) הצפוי מחשיפה. את L(k) אפשר להגדיר כמחיר החשיפה, כאשר המערכת (k) נמצאת בפעולה.

אפשר לחשב את האובדן הכולל L(k) אם ניקח בחשבון את כל האיומים האפשריים, כאשר האיומים הם נתיבי כניסה לנכסים מוגנים כמו:

L(k) = Σ [(ערך החשיפה) x (הסתברות תקלה באמצעי ההגנה)]

הקשיים שנובעים מגישה זו קשורים לאפשרות של זיהוי וכימות כל מסלולי הכניסה האפשריים לנכסים, ולאפשרות להעריך את הסיכויים לתקלה במנגנוני ההגנה שחוסמים מסלולים אלה. גישה זו מעודדת מנהלי סיכונים לערוך, ללא הצדקה, חישובים מדויקים יתר על המידה. לדוגמה, דיון ממושך בשאלה אם החשיפה תגרום לאובדן של 73,000 שקל או של 83,900 שקל אינו רלוונטי, מכיוון שאין לכך חשיבות רבה (הערכים קרובים למדי).

סטיות קלות בערכים שנבחרו יכולים לתרום באופן משמעותי לזמן הנדרש לביצוע הערכת סיכונים, מבלי שהערך הנבחר יהיה מדויק מאוד. לכן, כדאי לנתח את הסיכון במונחים של סדרי חשיבות ולא במונחים של גודל הערך. כמו כן, יש להעריך באופן גס את ההסתברות להתרחשות האובדן. זו הגישה שמציע קורטניי, שמייעץ לשים דגש על הגודל היחסי של האובדן ועל ההסתברות שייתרחש, כמצויין בטבלה 8.2.

טבלה 8.2 פרמטרים לעלות האובדן ולתדירות המופע

ערך משוערך של האובדן	i	תדירות משוערת של המופע	f
10 שקלים	1	אחת ל-300 שנה	1
100 שקלים	2	אחת ל-30 שנה	2
1,000 שקלים	3	אחת ל-3 שנים	3
10,000 שקלים	4	אחת ל-100 יום	4
100,000 שקלים	5	אחת ל-10 ימים	5
1,000,000 שקלים	6	אחת ליום	6
10,000,000 שקלים	7	עשר פעמים ביום	7
100,000,000 שקלים	8	מאה פעמים ביום	8

8.4 ניתוח סיכונים לפי קורטניי

שני מרכיבים עיקריים בניתוח זה, המהווה הצהרה כמותית בכל אירוע אובדן אפשרי:

(1) העלות של התרחשות החשיפה מצוינת על ידי הפרמטר i.
(2) תדירות ההתרחשות מצוינת על ידי הפרמטר f.

התחומים של הפרמטרים i ו-f מצוינים בטבלה **8.2**. הם משמשים לחישוב אובדן שנתי צפוי לפי הנוסחה:

$$L = 1/3 \times 10^{(i+f-3)}$$

לדוגמה, אם אירוע בעל אובדן פוטנציאלי של **100,000** שקל בכל התרחשות צפוי להתרחש אחת לשלוש שנים, האובדן השנתי הצפוי הוא **33,333** שקל. אם נשתמש בנוסחה זו נקבל מטבלה **8.2** את הערכים $i=5$ ו-$f=3$, והנוסחה תהיה:

$$L = 1/3 \times 10^{(5+3-3)} = 1/3 \times 10^{5} = 33{,}333 \text{ שקל}$$

בעזרת הערכים i ו-f ניתן למצוא בטבלה **8.3** את ערך האובדן. הטבלה מראה רק ערכים מעוגלים של האובדן, מכיוון שהערכים i ו-f ששימשו לחישוב, אינם מדויקים.

טבלה 8.3 אובדן שנתי צפוי

ערך של i	ערך של f (קשור לתדירות ההתרחשות)							
	1	2	3	4	5	6	7	8
1				30	0.3K	3 K	30 K	0.3M
2				0.3K	3 K	30 K	0.3M	3 M
3			0.3K	3 K	30 K	0.3M	3 M	30 M
4		0.3K	3 K	30 K	0.3M	3 M		300 M
5	0.3K	3 K	30 K	0.3M	3 M			
6	3 K	30 K	0.3M	3 M				
7	30 K	0.3M	3 M					
8	0.3M	3 M						

שים לב! הערך של i קשור למחיר או להשפעה של האירוע.

חישוב האובדן השנתי הצפוי הוא מרכיב חשוב במתודולוגיה שמתוארת להלן בקווים כלליים:

(1) קבע צוות שיבצע את ניתוח הסיכונים. כדי לשקול בצורה נכונה את ההשפעה ואת הסיכויים, יש צורך בצוות רב-תחומי שיכיל נציגים בכירים ומנוסים של משתמשי הנתונים והבעלים, של מחלקת האבטחה, של הביקורת הפנימית ושל כל אגף במחלקת המחשב.
(2) ציין את כל המערכות היישומיות, בטופס הנראה בתרשים 8.2.
(3) פרט בטופס זה את כל קבצי הנתונים שמשמשים כל יישום.
(4) קבע ערכים להשפעה ולתדירות ההתרחשות בכל צומת בטבלה.
(5) חשב את הסיכון L בערכים של מחיר ליחידת זמן, לכל זוג ערכים שהוכנסו בסעיף 4.
(6) שקול שימוש באמצעי הגנה והחלט, לפי המידע המתקבל מסעיף (5), אם מחירו סביר ביחס לתועלת שניתן להפיק ממנו, ואם הוא עומד בקריטריונים הנמצאים בטבלה 8.4 (סלצר ושרודר, 1975; הופמן, 1977; פרקר 1981). בטבלה 8.5 ניתנים אמצעי הגנה טיפוסיים.

למרות העובדה שניתוח סיכונים כמותי המשתמש בטכניקות מקובלות יכול לספק מידע מועיל, אין לשכוח שהמספרים המתקבלים מבוססים, במידה רבה, על ניחוש. ניתוח סיכונים מותנה בהערכה סובייקטיבית שיעילותה תלוייה בידע ובניסיון של הגורם המעריך. על ניתוח הסיכונים לפי המידולוגיה של קורטניי נמתחה ביקורת מהסיבות הבאות:

(1) התהליך יקר ואינו מצדיק את מחירו (שוויצר, 1982).
(2) קשה מאוד לבחור ערכים, אפילו גסים, לפרמטרים i ו-f.
(3) מסובך מאוד להבין ולנבא את כל סוגי ההתקפות על מערכת המידע.
(4) המתודולוגיה אינה מספקת בסיס לבחירת אמצעי הגנה שיקטינו את הסיכון ובסיס להערכת ההשפעה שיש לאמצעי ההגנה על L, האובדן השנתי הצפוי (גלסמן, 1977).

שם של מערכת או קבוצת נתונים		לא מכוון			מכוון			חשיפה (פרצה) אם אינו מסוגל לפעול במשך: (שעות)					הערות
		חשיפה	שינוי	הרס	חשיפה	שינוי	הרס	2	4	8	12	18	
		סודיות	שלימות נתונים	נתונים	סודיות	שלימות נתונים	נתונים						
	i												
	f												
	L												
	i												
	f												
	L												
	i												
	f												
	L												

תרשים 8.2 גליון עבודה לניתוח סיכונים

טבלה 8.4 קריטריונים לבחירת אמצעי הגנה

קריטריונים לבחירה של אמצעי הגנה	הערות
(1) עיקרון עלות/תועלת	o לכל אמצעי הגנה יש מחיר. על ההחלטה שקשורה בעלות ההגנה לקחת בחשבון את ערך הנתונים ואת חובת המשתמש בנתונים להגן עליהם.
(2) האבטחה אינה תלויה בסודיות	o יש להניח שהעבריין הפוטנציאלי מודע להתקני ההגנה אך אין הוא יכול לנטרל אותם, מכיוון שהם פגיעים.
(3) הצורך לדעת, או ההרשאה הנמוכה ביותר	o יש לספק לאדם או להתקן, מידע מיזערי שיספיק לביצוע יעיל של הפונקציות הנדרשות מהעובד, או מההתקן.
(4) בקרה בלתי תלויה של האובייקטים המבוקרים	o על עובדים ומבקרים להבטיח שאמצעי ההגנה לא יהיו תלויים באנשים שמבוקרים על ידם.
(5) התערבות מינימלית	o אמצעי הגנה אידיאלי יפעל ללא התערבות של בני אדם.
(6) מוגן בפני תקלות	o במקרה של תקלה, המכשיר יוכל להמשיך לפעול.
(7) הוראות הפעלה אחידות	o הפעלת ההתקן צריכה להיות זהה בכל תחום פעילות שהוגדר עבורו.
(8) שלימות	התקן צריך להכנס לפעולה רק לאחר שנבדק.
(9) עמידות	o אמצעי ההגנה צריך לפעול באופן יעיל לאורך זמן (שים לב, ביצועי ההתקנים שתלויים בהתערבות, או בתמיכה חיצונית נוטים להתדרדר במשך הזמן)
(10) מקובל על המשתמש	o אם ההתקן מגביל את המשתמש באופן בלתי נסבל, סביר להניח שהמשתמש יעקוף אותו.
(11) פיקוח, ניטור	o התקן צריך לאפשר פיקוח על תקינות פעילותו, על תקלות ועל ההתקפות עליו.
(12) ניתן לביקורת	o יש לאפשר את בדיקת התקן ההגנה, כדי לבדוק אם הביצועים עומדים במפרט.
(13) אחריות	o רק אדם אחד יהיה אחראי על כל אמצעי ההגנה.
(14) תגובה להתקפה	o אמצעי הגנה טוב יגיב בטרם ייגרם נזק ממשי לנכס המוגן.

טבלה 8.5 דוגמאות טיפוסיות של איומים ואמצעי הגנה

האיום	אמצעי ההגנה
1. <u>אבטחת נתונים</u>	
איומים למידע היסטורי רגיש	מניעת היקש לוגי רישום פרטים של שאילתות
איומים למידע רגיש, בעל ערך	בקרת כניסה והגבלות, חציצה, היררכיה של הרשאות
2. <u>אבטחת מערכת ההפעלה</u>	
תקלות במערכת ההפעלה,	בדיקה וניסוי של מערכת ההפעלה
איומים מעובדים	רישום, נוהלי זיהוי ואימות, מטריצת בקרת כניסה
3. <u>אבטחה פיסית</u>	
הפרעות אלקטרוניות ואלקטומגנטית	הצפנה
פורצים	שומרים, סיסמאות, מנעולים, תגים ומפתחות
אסונות	בחירת אתר, תוכנית גיבוי, תוכנית התאוששות

8.5 שיטות היוריסטיות המשמשות ככלי עזר לניתוח סיכונים

קיימות בעיות רבות בפיתוח של תוכנית אבטחה לארגון. עלינו לדאוג לכך שיהיה בידינו ולו גם מידע מועט על איומים והשפעותיהם במצב מסוים. יכול להתקיים מצב שלא יובן במלואו, אך תמיד יהיו רסיסי מידע, תחושות והרגשות אנוש על מה שקורה. אסטרטגיות המשתמשות במידע חלקי קרויות אסטרטגיות "היוריסטיות". אין הן מבטיחות הצלחה, אך הן עדיפות על לא כלום.

טכניקה היוריסטית פשוטה היא רשימת התיוג (checklist). לעתים קרובות זוהי רשימת שאלות שלוקטה במשך הזמן על ידי כמה אנשי מקצוע, המצביעה על פרטים ותחומים הדורשים תשומת לב. אחוז ניכר מניתוח הסיכונים ניתן לביצוע בשיטות היוריסטיות, כמו למשל, רשימת התיוג. רשימות תיוג זמינות ורבות יכולות לסייע בפיתוח של תוכנית אבטחה (AFIPS, 1974; וורינג, 1978; דייויס ופרי, 1982).

לניתוח סיכונים וניתוח כללי יותר, המתבצע בזמן פיתוח מערכת המידע, משתמשים בשיטות היוריסטיות. בנוסף לרשימות התיוג ישנן טכניקות נוספות:

(1) שימוש באירועים שהתרחשו בעבר, כדי לנבא תקלות עתידיות באבטחה.
(2) להכיר בעובדה שאנשי המחשב הם בני אדם, ולכן:
   (א) בצד כישוריהם, יש להם גם חולשות.
   (ב) הם יוצרים פגיעויות בתוך תחום הפעילות שלהם.
(3) להכיר בעובדה שתקלה קשורה, לעתים קרובות, בתגובה חלקית לשינוי.

חוסר מיומנות, או מיומנות חלקית, של עובדים מחזקות את הצורך בתשומת לב מיוחדת למצבים שבהם חולשות של מתכננים באות לידי ביטוי. לדוגמה, יש לבדוק הנחות בסיסיות בתכנון האבטחה ובמישקים לתת מערכות. מתודולוגיית ניתוח החשיפה (פרקר ומדן, 1978; פרקר 1981) מכירה בחולשות של האנשים ובודקת את החשיפה לאובדן, ביחס למספר האנשים שיכולים לגרום להתרחשותו, במכוון ושלא במכוון. אפשר להשתמש במתודולגיה זו במצבים שבהם גישת קורטנייי אינה ישימה. בשיטה זו, מסווגים כל העובדים, מהבכיר ועד לזוטר ביותר, לפי מקצוע ולפי מיומנות. בדרך זו אפשר לקבל תחזית אמינה לאיומים מבפנים, ואמינה פחות לאיומים חיצוניים. יתרונה נובע מהעובדה שרוב האובדנים הידועים נגרמים על ידי עובדים שמלכתחילה ניתן בהם אמון.

כדי להתגבר על קשיים בתקופה של שינויים, יש לזהות מצבים

זמניים מסוג זה במערכות המידע. לאחר זיהוי מצבים אלה, יש לבדוק באיזו מידה מספקים נוהלי האבטחה הקשורים בהם. להלן, כמה דוגמאות:

* בזמן החלפת עובדים.
* תקופת ההתקנה של שינוים בתוכנה יישומית.
* המעבר מפעולה מלאה להפסקת פעולה.

אירועים מתועדים (פרקואר וונג, 1983) מצביעים על כך ששעות הבוקר המוקדמות הן הזמן הנפוץ ביותר להבערת אש. כמו כן, אפשר לראות שספרנים בספריות סרטים גורמים נזק לקבצים בעת הפסקת עבודתם. דוגמאות אלו מצביעות בבירור על הקשר שבין תקלה לשינוי.

השיטה של חיזוי תקלות עתידיות על פי תקלות קודמות נפוצה מאוד. לעתים קרובות, יודעים העובדים בבירור על בעיות מקומיות ועל סיכונים, כתוצאה מטיפול במקרים קודמים שבהם כמעט והתרחשה תקלה. לכן, כדאי לאסוף מידע כזה בשיטתיות בדרך של מילוי טפסים, שבהם ידווח על בעיות באבטחה. למרבה הצער, טפסי דיווח מהווים בעיה, מכיוון שאין אוהבים למלא דוחות מפורטים. טכניקה מוצלחת יותר היא טכניקת המקרה הקריטי (ספיר, 1976), שאינה דורשת מהצופה בתקלה למלא דוח רשמי מפורט על כל מקרה. טכניקה זו דורשת ממבצעי ניתוח הסיכונים לראיין את העובדים ולדלות מהם רק את המקרים החשובים לתיעוד.

אפשר לפתח את השיטה על ידי שימוש בניתוח תרחישים (scenario analysis) (פרקר, 1981). גישה זו יכולה להחליף את גישת קורטניי במצבים שבהם אי אפשר לקבוע באופן אמין את סיכויי ההתרחשות של אירועים. תרחישים יכולים להיות אירועים אמיתיים קודמים, או אירועים מדומים. ניתוח התרחישים סובייקטיבי מאוד ומקביל לגישת קורטניי, אך הוא מרחיק לכת בעזרה ישירה לבחירת אמצעי הגנה. ניתוח התרחישים בנוי מהשלבים הבאים:

(1) לכל איום יוכן תרחיש אחד, או כמה תרחישים, שמתארים כיצד הנכס, או הנכסים, יכולים להפגע ולגרום לאובדן.
(2) מנהלי המחלקות מקבלים את התרחישים הרלוונטיים.
(3) המנהלים בוחנים את התרחישים, דוחים חלק מהם ומתקנים את השאר.
(4) על סמך ההערות, מתקנים את התרחישים ועורכים אותם בהתאמה, כקלט לשלב 1.
(5) חוזרים על שלבים 1 עד 4, עד שמתקבלים תרחישים שימושיים והגיוניים, שהמנהלים מאמינים שהם מייצגים פגיעויות משמעותיות. בניתוח התרחישים נכללים גם הפרטים הבאים:

(א) ההגנה הנוכחית.
(ב) שיפורים מוצעים באמצעי ההגנה.
(ג) נקודות תורפה.

(6) בוחרים במנגנוני הגנה מתאימים. התרחישים, ביחד עם מנגנוני ההגנה הנבחרים, משמשים לבדיקת יעילות חוזרת של אמצעי ההגנה. היתרון של ניתוח התרחישים נובע מכך שהוא מהווה כלי עזר מצוין לתקשורת בין גישות שונות המעורבות בחקר האבטחה.

8.6 בדיקת האבטחה בארגון או ייזום תוכנית אבטחה

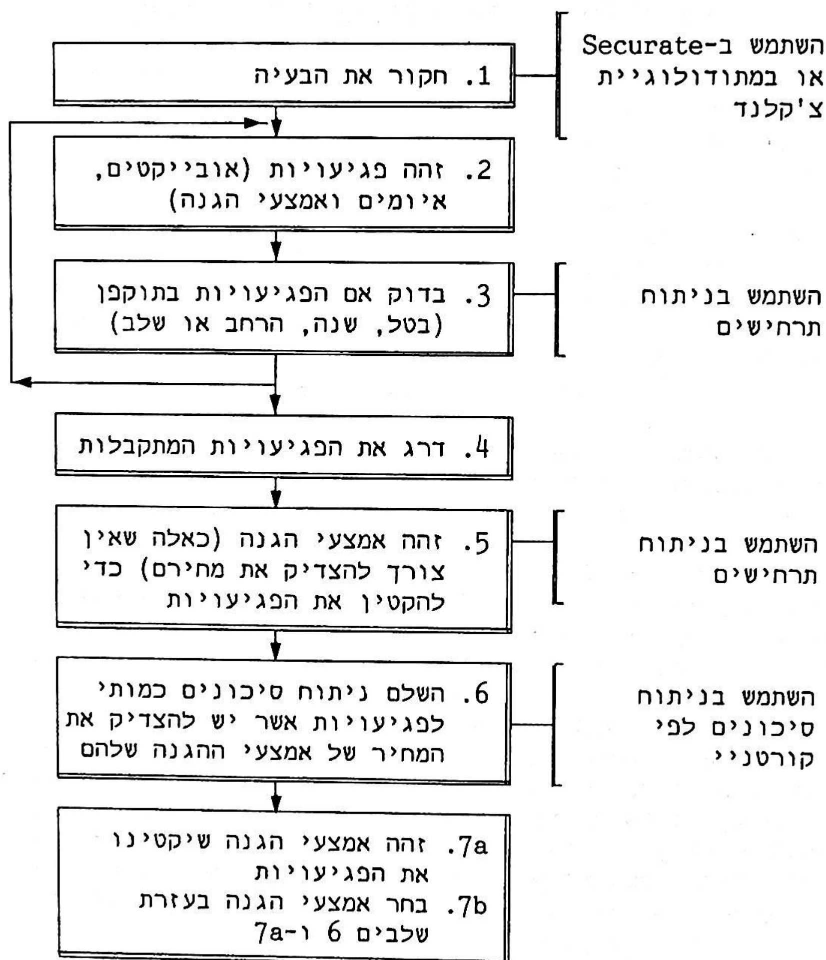
רשימות תיוג, כבסיס לבדיקת האבטחה, נפוצות למדי ומשמשות כלי עזר יעיל מאוד. חסרונן הוא ביצירת אשליה של בדיקה יסודית שעלולה להסתיר בעיות אמיתיות. בדיקה פשוטה בעזרת רשימות תיוג אינה מספקת, מכיוון שתשומת הלב מופנית, בדרך כלל, לקבוצה צרה מדי של פגיעויות וכתוצאה, אמצעי ההגנה המותקנים אינם מספיקים. תוכנית האבטחה תלויה באנשים, שלא ניתן לנבא את התנהגותם ברמה סבירה של בטחון. לכן, כאשר בודקים אבטחה של מערכות מידע, או יוזמים תוכנית אבטחה, חובה להשתמש בשילוב של גישות. כך אפשר להגיע לבדיקה כוללת (הוליסטית), שלוקחת בחשבון את העובדה שאבטחה היא דבר המשתנה בהתמדה כתוצאה מנוכחות בני אדם ומהתפתחות הטכנולוגיה.

בתרשים 8.3 מתוארת מתודולוגיה לייזום תוכנית אבטחה. בבדיקת אבטחה קיימת, יש להשתמש רק בשלושת השלבים הראשונים של המתודולוגיה, אך אם האבטחה לקויה, יש להשתמש בכל השלבים.

אפשר להגיע לבדיקה כוללת (הוליסטית) על ידי שימוש במתודולוגיית צ'קלנד (צ'קלנד, 1981), שמתוארת בתרשים 8.4. מטרת מתודולוגיה זו היא ליצור מערכת היפותטית מושלמת ולהשוות אותה עם המערכת האמיתית, כדי לזהות נקודות טעונות שיפור (ראה גם תרשים 8.5). השלבים האחרונים של מתודולוגיית צ'קלנד ישתלבו עם הנוהל המתואר בתרשים 8.3. באופן זה יוצרת מתודולוגיית צ'קלנד מסגרת שבתוכה אפשר לארגן את המחקר ולעודד בדיקה של נקודות חשובות. גישה זו אינה נותנת את התשובה הנכונה באופן ישיר, אך היא עוזרת לחשוף מה קורה על ידי הצבת שאלות פתוחות שלהן תשובות אפשריות רבות. חשיבות רבה לדבר, כי אבטחה טובה דורשת שילוב של אמצעי הגנה טכנולוגיים, מנהליים ופיסיים.

דרך נוספת לביצוע בדיקה היא ע"י שימוש ב-Securate (הופמן, 1977) שהיא מערכת תוכנה להערכה וניתוח של מתקן מחשב. המודל שלפיו היא בנויה מחלק את המתקן למערכת של שלשות,

נכס-איום-אמצעי הגנה (Ai, Tj, Sk בהתאמה). לכל נכס (A) יש ערך אובדן, לכל איום (T) יש סבירות ולכל אמצעי הגנה (S) יש התנגדות. הערכים מבוססים על תיאורית הקבוצה הנסתרת (fuzzy set theory), כדי שאפשר לסווג את רמת האבטחה במתקן ובמחלקות המשנה שלו. בעזרת מקבל החלטות אנושי, יש ל-Securate סיכוי להשלים בדיקה של האבטחה. עם זאת, הניסיון הוכיח שהמערכת עוזרת להבין את אבטחת המתקן וממקדת את המחשבות למסגרת מוגדרת היטב, שמאפשרת למנהלים לראות את המצב בצורה ברורה יותר ולהבין אותו לעומק (הופמן ואחרים, 1978).



תרשים 8.3 מתודולוגיה לייזום מערך אבטחה בתוך הארגון

תרשים 8.4 סכימה של מתודולוגיית צ'קלנד

תרשים 8.5 השוואה בין מערכת אבטחה תיאורטית לבין המערכת הקיימת

א. מערכת האבטחה הקיימת
ב. מערכת אבטחה תיאורטית

התוצאה הסופית של הבדיקה תהיה שלשות (Sk ,Tj ,Ai) המייצגות פגיעויות שונות. חלק מהפגיעויות יכולות להיות קשורות לנכס, או לאיום אחד. הפגיעויות נבדקות בעזרת ניתוח תרחישים ולאחר שיבוצעו שינויים, הן יסווגו לפי גודל הסיכון. בשלב ראשון, יש למצוא אמצעי הגנה לפגיעויות שאין צורך להצדיק את עלות אמצעי ההגנה נגדן. בשלב שני, יש לבצע ניתוח סיכונים כמותי לשאר קבוצות הפגיעויות, שקשה להצדיק אמצעי הגנה נגדן, מכיוון שהם אינם יעילים במידה מספקת ו/או יקרים מדי.

8.7 תכנון לשעת חירום

על אף שננקטו אמצעי זהירות ונוהלי אבטחה קפדניים, לא ניתן להסיר לחלוטין את הסיכון ועל כן, שיבושים עלולים תמיד להתרחש. המטרה של תכנון לשעת חירום היא לנקוט פעולה מיידית בעת שתתרחש הפרעה לשירותי המחשוב שתבטיח התאוששות מהירה ואובדן מינימלי.

מצב חירום הוא הפרעה בלתי צפויה לשירותי המחשוב, שדורשת אמצעי נגד שאינם נמצאים בשימוש שגרתי. קיים מגוון רחב של מצבי חירום, החל מהפרעה שולית לאספקת החשמל ועד לאסון טבע, כמו הצפה או אש. מצבי חירום אחרים יכולים להגרם מפיצוץ, מתקלה בחומרה, מתקלות בתוכנה, מתקלה במיזוג האוויר ומפעולות של אנשי יחידת המחשב, כמו השבתה וכדומה. קל יותר להתגבר על אירוע כזה אם יתקיימו נוהלים מתועדים והגיוניים שתורגלו בהצלחה. אי אפשר להתכונן לכל האירועים, אך עם זאת, תוכנית לשעת חירום חייבת להכיל את הפרטים הבאים:

(1) נוהלים מוכנים מראש (standby) להפעלה לאחר שהתרחשה הפרעה לפעולה הרגילה.
(2) נוהלי התאוששות לאחר שגורם ההפרעה זוהה ותוקן.
(3) חלוקת האחריות בין העובדים לביצוע סעיפים 1 ו-2 (ברודבנט, 1979; פרידמן, 1982).

הגדרת תחומי האחריות במקרה של הפרעה הוא המאפיין הראשון, ואולי החשוב ביותר, של תוכנית לשעת חירום. לצורך זה יש למנות מתאם, או מנהל, שיכנס לתפקידו בעת חירום ויחליט על הפעולות שיתבצעו. מכיוון שהפעולות כוללות האצלת סמכויות וקביעת תחומי אחריות לחברים בקבוצת האישוש, חייבת להיות למתאם הפעולות גישה לשמות, למספרי טלפון ולכתובות, כדי שיוכל להזעיק את חברי הקבוצה. סביר להניח שהתוכנית תהיה מפורטת באופן חלקי בלבד ולא תכלול את כל האירועים האפשריים. לכן, מתאם הפעולות צריך לסמוך על חברי הקבוצה ולהטיל עליהם את האחריות לביצוע ההתאוששות, לפי הנהלים הקיימים, אך אל לו להכנס לפרטים.

מאפיינים נוספים של תוכנית לשעת חירום:

* הסדרי גיבוי הדדיים עם יחידות מחשב אחרות.
* רשימת התפקידים החשובים ואלה שאפשר לוותר עליהם בשעת חירום.
* מערכת כיבוי ידנית (manual fall-back system) לצורך הפעלה במהלך הפסקות קצרות באספקת החשמל.
* חברות בתוכנית להגנה בפני אסונות. לעתים קרובות, לאחר אסון יכולים ארגונים להחליף את החומרה בקלות יחסית, אך בניה מחדש, ואף שיפוץ, של המתקנים האחרים עלול להיות ממושך ביותר. פתרון לבעיה זו ישמש חוזה שייחתם בין הארגון לבין חברה מתאימה לאספקת אולם ריק ושירותי עזר, בשעת הצורך.

ללא קשר לשאלה אם התוכנית לשעת חירום מתועדת היטב, חיוני לתרגל חלקים ממנה לפני שיתרחש אסון אמיתי וכך להבטיח את יעילותה ולהכין את הצוות לפעולה. ארגונים המחזיקים בתוכנית מתוכננת היטב לשעת חירום, בדקו אותה על ידי "סגירת" מרכז המחשבים הרגיל ומתן הוראה לצוות שמחוץ למרכז להפעיל את השירותים לשעת חירום. בעיות שצצו בגלל דברים פעוטים, כמו מחסור בטפסים, או הוראות הפעלה והנחיות למשתמש שאינן מעודכנות, זכו באופן זה לפתרון. יש לבדוק ולתרגל, מדי פעם, את כל ההיבטים הקשורים לתוכנית לשעת חירום ולעדכנם כפי הצורך.

עדכון חיוני נוסף מתייחס למערכות מידע חדשות. על הצרכים לשעת חירום של כל מערכת יישומית חדשה להיות חלק מתהליך התכנון ולכן - גם חלק ממפרט המערכת.

8.8 סיכום

אי אפשר לפתח תוכנית אבטחה זהה עבור שתי סביבות מחשוב שונות. לכן, יש להכין הערכה נפרדת לכל ארגון ולכל מערכת מידע בתוך הארגון, כדי לקבוע מהי אסטרטגיית ההגנה הטובה ביותר. יש להתייחס לאבטחה עוד בשלב תכנון מערכת המידע, משום שקשה, יקר ולעתים גם אי אפשר, להגן על מערכת שתוכננה והותקנה ללא אמצעי הגנה. בפרק זה הוצגו כמה טכניקות ומתודולגיות לפיתוח ולבדיקה של תוכנית אבטחה בתוך הארגון. אפשר להשתמש בטכניקות אלו בשלב התכנון של מערכת המידע.

הקושי ביישום ניתוח סיכונים כמותי איננו רק במתן ערך כספי מדויק לאיום. במקרים מסוימים, בנושאים חברתיים, אי אפשר וגם אין רוצים למדוד איומים ופגיעות במונחים של נזק כספי, כמו

לדוגמה, במקרה של חשיפת רשומות רפואיות סודיות. הערכה של תדירות ההתרחשות קשה במידה שווה. אסונות טבע, כמו הצפות, נחקרים ונלמדים זמן ממושך ולכן קיים לגביהם מידע נרחב ובעל ערך סטטיסטי. לעומתם, האיומים בתחום המחשוב חדשים יחסית ואינם אחידים. מסיבות אלו, לא נאגר עדיין מידע סטטיסטי שימושי ומספק על האיומים השונים. מומלץ לנקוט בניתוח הסיכונים המספרי באופן סלקטיבי, ורק לאחר השימוש בשיטות איכותיות. לפי עיקרון פרטו (Pareto principle), חלק קטן מהסיכונים הצפויים בסביבה עסקית, מהווים את רובו של הסיכון האפשרי. לכן, יש לנקוט לגבי סיכונים אלה בניתוח סיכונים מקיף.

מתודולוגיית הפיתוח שהוצגה בפרק זה נוקטת בשילוב של טכניקות כמותיות ואיכותיות. בעזרתה אפשר להבין את המתקן ולשלב, באופן הנכון ביותר אמצעי הגנה טכניים, מנהליים ופיסיים.

על אף השימוש בכל אמצעי ההגנה, השיבושים הם בלתי נמנעים. תוכנית לשעת חירום תקטין את הנזק, אך קיימים מצבים שעלולים לסכן את הארגון עצמו. היכולת של הארגון להמשיך לפעול נמצאת באחריות המנהלים הבכירים בחברה (ליין, 1985). בתהליך שנמצא בעיצומו הופכים ארגונים רבים לתלויים במחשבים בפעילותם השוטפת ואף על פי כן, חלק מאותם ארגונים עדיין אינם משתמשים באמצעי זהירות ובתוכנית לשעת חירום, בניתוח מקדים ובהכנות מתאימות למקרה של שיבושים.

שאלות

8.1 ארגון התלוי במחשבים שלו, חוקר את הסיכונים שהוא חשוף להם: תקרית אש, שתתרחש אחת ל-300 שנה, תגרום ל-100% אובדן מיכולת המחשוב, בערך כולל של מיליון שקל; הצפה, שתתרחש אחת ל-30 שנה, תגרום ל-10% אובדן. חשב את האובדן השנתי הצפוי מאש ומהצפה בעזרת שיטת החישוב שלך ובעזרת שיטת קורטניי. הסבר את ההבדלים בין שתי התשובות.

8.2 קשה לפתח אסטרטגיית אבטחה למערכות המידע בארגון. האם לדעתך צריך פיתוח תוכנית האבטחה להיות באחריות של מנהלי תחום עיבוד הנתונים?

8.3 הסבר את המשמעות והתועלת שבשיטות ההיוריסטיות, מצב זמני וניבוי של תקלות עתידיות על פי מצבים קודמים. ציין כמה דוגמאות.

8.4 מנכ"ל מדווח שארגונו השקיע 80,000 שקל בתוכנית הגנה המבוססת על ניתוח סיכונים מלא. הוא מאמין שתרגול אינו הכרחי, מכיוון שהוא מפריע לפעילות השגרתית. מה דעתך?

פרק 9

תחיקה לאבטחת פרטיות והגנת נתונים

האיום השנוי ביותר במחלוקת למערכות מידע המבוססות על מחשב הוא אבטחת הפרטיות. אפשר להתגבר על איום זה בעזרת אמצעי הגנה טכניים, מנהליים ותחיקתיים. בפרק זה נסקור גישות לפרטיות, כבסיס לבדיקת התחיקה בנושא הגנת נתונים. במדינות מתקדמות קיימת הכרה בחיוניות התחיקה, אך ישנם הבדלי השקפות לגבי תוכנו ואופיו הכללי של החוק. כל תחיקה בנושא זה תשפיע על ניתוח ותכנון מערכות מחשוב. נסקור אירועים שהתרחשו בבריטניה, שיאפשרו להעריך את המצב התחיקתי שבו אנו נמצאים כיום ואת ההתפתחויות הצפויות בנושא זה. למרות שבחרנו לשים דגש על אירועים שהתרחשו בבריטניה, קיים בנושאים אלה עניין בינלאומי, כי "סדנא דארעא חד הוא".

לעניין התחיקה והמצב המשפטי בישראל, עיין ב"**נספח א - מערכות מידע ממוחשבות והמשפט בישראל**". חומר נוסף תמצא בכתבי עת למחשוב ובעיתונות המקצועית והכללית, כפי שמפורט ברשימה הביבליוגרפית.

9.1 גישות לפרטיות והשפעתן על טכנולוגיית המידע

למרות קדושת עיקרון הפרטיות בעולם החופשי, קשה להגדיר אותו במסגרת חוק פשוט הניתן לאכיפה. בוועידה הראשונה בנושא פרטיות, שהתכנסה בשוודיה בשנת 1967, נשמעה המסקנה שפרטיות היא זכות בסיסית ושכל המדינות צריכות לחוקק חוקים שיגנו עליה. קביעה בסיסית בהגדרת הפרטיות היא הזכות למנוע מגורמים זרים לדעת פרטים מסוימים על חייו של הפרט. מאידך, למדינות מודרניות זכות לגיטימית לדרוש מידע מאזרחים, מכיון שאין זה אפשרי לנהל את שירותיה החברתיים של הממשלה, כמו שירותי הבריאות והחינוך ללא מידע אישי מתאים. יתר על כן, שמירה על הסדר האזרחי והביטחון הלאומי מחייבת גישה למידע אישי. לכן, הקושי העיקרי הוא להגן על פרטיות האנשים, או של קבוצות אנשים ובו זמנית, לאפשר למדינה לבצע את משימותיה הלגיטימיות. אם מקבלים את ההנחה שיש להגביל את חירות האדם באופנים רבים לטובת הקהילה, אפשר לנסח עקרונות לטיפול נכון בנתונים אישיים (וור, 1973; ליניאס, 1977).

בטבלה 9.1 מוצגים עקרונות טיפוסיים, שמקובלים על הממשלות במדינות החופשיות. אולם, מסיבות שונות, כאשר הנושא של פרטיות משולב עם מחשבים, מתעורר ויכוח.

טבלה 9.1 עקרונות לטיפול נכון בנתונים אישיים

(1) פתיחות	אסור שתהיינה מערכות סודיות המכילות נתונים אישיים.
(2) גישה על ידי נשוא הנתונים	לכל אזרח הזכות לדעת איזה מידע מוחזק אודותיו ולאיזו מטרה הוא משמש.
(3) הגבלת השימוש	לכל אזרח זכות למנוע שמידע הנאסף למטרה אחת ישמש למטרות אחרות, ללא הסכמתו.
(4) שיתוף נשוא הנתונים	חייבים להיות נוהלים שיאפשרו לאזרח לשנות, או לתקן נתונים שנוגעים לו.
(5) אחריות של המשתמש בנתונים	ארגון המפעיל מערכות של נתונים אישיים אחראי לאמינות הנתונים ולשימוש בהם.

המידע המוחזק במערכות ידניות זהה לזה שנמצא במערכות מידע המבוססות על מחשב. ההבדל העקרוני הוא ביכולת העיבוד של מערכות מידע המבוססות על מחשב, כמתואר בטבלה 9.2. ההבדל טמון בעובדה שמחשבים מאפשרים לארגונים לאסוף כמויות עצומות של מידע על אנשים, בעוד שמערכת ידנית אינה מסוגלת לטפל בכמות כזו לצורך ביצוע אחזור, חיפוש, מיון, שיווק, ניתוח וכו'. חוסר היעילות והמגבלות הטבעיות של מערכות ידניות, מהוות הגנה על הפרטיות. המחשבים נותנים בידי המשתמשים אמצעים רבי עוצמה לטיפול בנתונים. בנוסף לכך, ניתן לשלבם ברשתות ארציות ובינלאומיות, ובכך להפיץ את המידע על פני איזורים גיאוגרפיים גדולים. גופים רבים אוספים מידע אישי ומאחסנים אותו במחשביהם וכתוצאה, נאגר מידע כמעט על כל אזרח. אין פלא איפוא, שהעניין מעורר דאגה מסיבות שונות:

(1) היקף: נאספת כמות גדולה של נתונים אישיים.
(2) החוסר בשלימות: קיימות הוכחות שלעתים קרובות מתבצע עיבוד של מידע לא שלם ולא מדויק.
(3) אין הגנה: מחסור באמצעי הגנה גורם לסיכון רב.

(4) אין מעורבות של נשוא הנתונים: נשוא הנתונים הוא אדם שנתוניו האישיים נמצאים בתהליך העיבוד; לעתים קרובות, המידע מועבר מיישום אחד למשנהו, ואפילו מארגון אחד למשנהו, ללא הסכמתו וללא ידיעתו של נשוא הנתונים.

אם משווים את ארבעת המאפיינים האלה עם העקרונות שנסקרו בטבלה 9.1, ברור שיש מקום לדאגה.

9.2 פעילות ציבורית ומשפטית להגנה על הפרטיות

ניתוח הפעילות שהתקיימה בשנות ה-70 וה-80 בבריטניה, עוזר לנתח את הצעות החוק השונות ולהעריך את האמצעים התחיקתיים שיהיו נחוצים בעתיד.

טבלה 9.2 השוואה בין מערכות ידניות לבין מערכות המבוססות על מחשב - עיבוד של נתונים אישיים

הגורם	מערכות ידניות	מערכות ממוחשבות
השפעה של קבצים גדולים רבים	האטה של התהליך. החקירה עלולה להיות איטית ובלתי מעשית	השפעה מעטה
מהירות תגובה	איטית באופן יחסי	מהירה
יכולת לבצע הצלבות תוך קישור בין קבצים שונים	קשה מאוד	פשוטה באופן יחסי
מרחק של חוקר הנתונים	המרחק מקטין את יכולת ביצוע החקירה	המרחק אינו משמעותי

הצורך בתחיקה בנושא הפרטיות נידון בבריטניה לפני כמעט 20 שנה. הויכוח עורר הדים בכמה מדינות, במיוחד בצפון אמריקה ובמערב אירופה. מדינות ספורות, ובריטניה אינה ביניהן, העבירו בשנות ה-70 חוקים הנוגעים להגנת נתונים. בתחילת שנות ה-80 נמנתה בריטניה על קבוצה קטנה של מדינות מתקדמות שלא חוקקו חוקים להגנה על פרטיות, למרות שהופעל עליה לחץ כבד מכמה מקורות:

(1) חברי הפרלמנט.
(2) קבוצות לחץ, כמו האגודה לזכויות האזרח.
(3) דוחות שהממשלה יזמה (כמו דוח יונגר ודוח לינדופ).
(4) ארגונים עסקיים שדאגו פן היעדר תחיקה בנושא הפרטיות יעמידם בעמדה עסקית נחותה, בהשוואה למדינות שבהן יש חקיקה מתאימה בנושא זה.

9.2.1 דוח יונגר

בשנים 1970 - 1972, בחנה ועדת יונגר את נושא הפרטיות. כאשר כתב המינוי שלה הגביל את פעילותה לסקטור הפרטי בלבד. ההיבטים של הפרטיות שנחקרו על ידה:

(1) פרסום ללא רשות (באמצעי התקשורת השונים וטלוויזיה).
(2) ניצול לרעה של פרטים אישיים.
(3) חדירה לחיים הפרטיים.
(4) גניבה של סודות עסקיים.
(5) התפתחויות טכנולוגיות (כולל אמצעי מעקב ומחשבים).

רק חלק מחקירה זו התמקד בהשלכות של מערכות מידע ממוחשבות.

טבלה 9.3 דוגמאות של תחיקה במדינות שונות בנושא הפרטיות

המדינה	החוק	שנה
שוודיה	חוק המידע (Data Act)	1973
ארה"ב	חוק הפרטיות (Privacy Act)	1974
גרמניה המערבית	חוק המידע הפדרלי (Federal Date Act)	1977
קנדה	חוק זכויות האזרח (Human Rights Act)	1977
צרפת	חוק עיבוד הנתונים והחרות (Data Processing and Freedom act)	1978
נורווגיה	חוק לרישום פרטים אישיים	1978
ישראל	חוק הגנת הפרטיות (התשמ"א) תקנות הגנת הפרטיות (התשמ"ו) תזכיר חוק המחשבים (התשמ"ז)	1981 1986 1987

טבלה 9.4 המלצות של דוח יונגר המתייחסות למחשבים

(1)	לשמור מידע למטרה מסוימת בלבד.
(2)	לאפשר כניסה למשתמשים מורשים רק לצורך המטרה שלשמה סופק המידע.
(3)	על כמות המידע שתאסף להיות קטנה ככל האפשר, בהתאמה לצרכים של המטרה המסוימת.
(4)	מידע לצרכים סטטיסטיים צריך להישמר באופן שבו הפרטים המזהים יהיו נפרדים משאר הנתונים.
(5)	להודיע לנשוא הנתונים על המידע שמוחזק אודותיו.
(6)	לציין משך זמן מירבי לשמירת הנתונים.
(7)	לקיים נוהלים לתיקון ולעדכון הנתונים.
(8)	לנטר מערכות, כדי לגלות ולטפל בהפרה אפשרית.
(9)	לבקר החלטות הנוגעות לאופן קידוד הנתונים.

המלצות ועדת יונגר מפורטות בטבלה 9.4. הדוח עורר תגובות מעורבות, בעיקר בגלל ההצעה שהמשתמשים ימלאו אחר ההמלצות מרצונם ולא מתוך חובה. הדוח המליץ שהחקירה תורחב לסקטור הציבורי ותרומתו העיקרית היתה בסלילת הדרך לוועדת לינדופ.

9.2.2 דוח לינדופ

בניגוד להמלצות ועדת יונגר, התרכז דוח לינדופ במערכות מידע המבוססות על מחשב. ב-1975 הודיעה הממשלה הבריטית על כוונתה לחוקק חוק להגנת נתונים ולהקים רשות סטטוטורית להגנת נתונים (Cmnd 6353, 1975). הוקמה וועדה בראשות סר נורמן לינדופ, שתפקידה היה לייעץ לממשלה בנושא התחיקה. לאחר עבודה ראשונית של הגדרת משמעות הפרטיות, החליטה וועדת לינדופ שהנושא הבסיסי הוא פרטיות הנתונים, לפיו מחזיק האדם בזכות לשלוט בתפוצה של מידע הנוגע לו (מולר, 1971; ווסטין, 1972).

הדוח הסופי מכיל פרק נפרד שעוסק בכל אחד מהתחומים שטופלו:

* ממשלה
* חינוך ותעסוקה
* שירותי הבריאות
* מזהה אישי ייחודי
* משטרה ושירותי בטחון

טבלה 9.5 נקודות חשובות מתוך דוח לינדוף לגבי מרכיבים עיקריים של החוק להגנת הנתונים

נשוא הנתונים	
1. צריך לדעת	א. מהו המידע שמוחזק עליו ב. לאיזו מטרה ג. מי ישתמש בו
2. תהיה לו אפשרות לבדוק	א. שהמידע מדויק ב. שרק מידע רלוונטי משמש את המטרה המוגדרת.
הרשות להגנת נתונים	
1. יש להקים את הרשות, שתנסח כללי עבודה לקבוצות שונות של יישומים העוסקים בעיבוד נתונים אישיים 2. הכללים צריכים להפוך לחוקים ולקבל תוקף חוקי	
היקף היישום	
1. על כל היישומים המעבדים פרטים אישיים בסקטור הפרטי והציבורי להרשם ברשות להגנת נתונים. 2. על כל הרשומות ה"קשות" (כמו עובדות פליליות) והקשורות במידע מודיעיני להיות תחת פיקוח החוק, מלבד מידע שקשור באופן ישיר לבטחון לאומי. 3. רשימת היישומים המפורטת ואופן השימוש בנתונים צריכים להיות פתוחה לעיון הציבור.	
מקרים מיוחדים	
1. לפי הוראת הרשות, חלקים מהרישום לא יהיו פתוחים לעיון הציבור. 2. לרשם הנתונים המוסמך מטעם המדינה תהיה סמכות להעניק פטור מרישום ברשות. כלל זה צריך להיות מוגבל ליישומים שקשורים בבטחון לאומי.	

הדוח, שהושלם ב-1978 (חלק מהצעותיו העיקריות מוצגות בטבלה 9.5), התחשב בקושי לשמור על איזון בין דרישות הפרטיות לבין הדרישות הלגיטימיות של הארגונים. שימוש במזהה אישי ייחודי לכל מטרה אינו אהוב, ולכן הדוח מנסה ליצור מסגרת שלא תכיל

מגבלות לא הגיוניות, או כאלו שמציבות דרישות מיוחדות למשתמשי הנתונים (Cmnd 7341, 1978). הוצע להקים את הרשות להגנת נתונים והוגדרו ההרכב והתפקיד של גוף זה.

גם הפעם הגיבה הממשלה בשלילה. אחת הטענות נגד הדוח היתה שההצעה בדבר כללי השימוש תגרום להרחבה משמעותית של החקיקה הפלילית.

9.2.3 פעילות בין השנים 1978 ל-1984

למורת רוחם של ארגונים רבים, לא נטו הממשלות שקמו אחרי הגשת דוח לינדופ להביאו לכלל חקיקה, כי חששו שהגנת נתונים יעילה תהיה יקרה לתפעול. אך הנסיבות השתנו מאז. בתקופת הכנת דוח לינדופ, נשען רובו של שוק המחשבים על מחשבים גדולים ששימשו ארגונים גדולים. מאז מתרחשת חדירה מסיבית של מחשבי מיני ומיקרו הגורמת לשינויים משמעותיים, שאינם מקלים על יישום עקרונות הגנת הנתונים.

9.3 הזירה הבינלאומית

עד לפרסום דוח לינדופ, העבירו מדינות רבות חוקים בנושא הגנת נתונים (ראה טבלה 9.3) ונוסחה אמנה כלל-אירופאית לנושא הגנת נתונים. מטרתה היתה להגן על הזכויות והחירויות הבסיסיות של האדם, כולל הזכות לפרטיות. בין סעיפיה:

סעיף 3 - האמנה מתייחסת לסקטור הפרטי והציבורי (המדינה תוכל לדרוש חריגים).

סעיף 9 - חריגים ינתנו רק כדי לשמור על:

* הסדר הציבורי
* בטחון המדינה
* עניינים כספיים של המדינה
* מצבים דומים

סעיף 12- החותמים על האמנה לא יפריעו לזרימת המידע בינם לבין חותמים אחרים.

על מדינות אירופה מופעל כעת לחץ הולך וגובר לאשרור האמנה.

9.4 נקודות למחשבה

בכל מדינה שבה נבדקה הגנת הנתונים באופן יסודי, התעורר ויכוח בשני נושאים מרכזיים. הראשון מתייחס לכללים הנכונים לעיבוד נתונים אישיים, והשני עוסק בזיהוי הארגונים שנתונים כאלה חיוניים עבורם, כמו המשטרה, שירותי הרפואה, השירות הציבורי ושירותי הבטחון.

חלק נכבד מהמידע המוחזק בארגונים אלה הוא רגיש, מכיוון שחשיפה לא מבוקרת של פרטי מידע מסוימים יכולה להשפיע על מוניטין של אדם, על העסקתו ו/או על חייו המשפחתיים. לאדם המספק מידע לארגון חשוב שהנתונים ישמרו במקום בטוח; לדעת מי רשאי לגשת לנתונים ואם הם נשמרים במדויק ואמינים. בדרך כלל, כאשר אותו אדם מבקש לראות את המידע המוחזק עליו, נאמר לו שהמידע חסוי. קיימת בכך סתירה: האדם היחיד שאינו יכול לראות את הנתונים הוא נשוא הנתונים עצמו, היחיד שעלול להפגע מחשיפתם (רול, 1974).

שירותי הבטחון מהווים תמיד מוקד לוויכוח בשאלת הסודיות. אי אפשר לדעת על פעולותיהם, גם באמצעות שאילתות בפרלמנט. דוגמה ליכולת של שירותי הבטחון לשמור על סודיות, תשמש העובדה שבין השנים 1978 - 1982 הצליחו שירותי הבטחון להסתיר התקנת מחשב לעבודה מקוונת עם שטחי אחסנה של 20GB, שיכול לשמור נתונים על מיליוני אנשים (סימונס, 1982). הרפתקה זו, שמטרתה היתה להקים מערכת מחשב מקיפה וסודית ל-M15 (הגוף המטפל בבטחון פנים), התרחשה (למרבה האירוניה) במהלך הויכוח על דוח לינדופ והתוכניות לא היו ידועות לפרלמנט. במצבים סודיים, מידע לא מדויק, או בלתי רלוונטי, עלול לגרום נזק בלתי הפיך לאזרח התמים (BBC, 1981).

טכנולוגיית המחשבים עזרה מאוד לשירותי הבטחון והמשטרה. המשטרה אוגרת מידע משני סוגים: עובדות מוכחות ("קשות") ומידע מודיעיני (Cmnd 7341, 1978). שני סוגי מידע אלה מאיימים על הפרטיות. המידע המודיעיני, הסובייקטיבי מטבעו, מדאיג במיוחד. סכנה גדולה במיוחד טמונה בעירוב שני סוגי המידע, ללא אבחנה. (בניין, 1979). האגף המיוחד הוא זרוע של המשטרה, אך אין חוק שיכול להגביל את המידע הפוליטי שאגף זה יכול לאסוף בהסתר. כל חברה מעניקה למשטרה עוצמה וזכויות יתר. יתר על כן, קיימות הוכחות, במדינות מכל גווני הקשת הפוליטית, שעוצמה זו, ללא אמצעי הגנה הולמים, מנוצלת לעתים לרעה.

9.5 התחיקה

הצעת החוק להגנת נתונים הונחה על שולחן הפרלמנט האנגלי ביוני 1983 והיו לה שתי מטרות:

(1) להגן על נשוא הנתונים מהאיומים הבאים:
(א) שימוש תקין במידע שגוי.
(ב) שימוש לא תקין במידע נכון.
(2) למלא אחר דרישות האמנה האירופאית להגנת נתונים, כדי לאפשר לתעשייה הבריטית לסחור בחופשיות.

בשנה שלאחריה נחקק החוק להגנת נתונים. בעקבותיו, נקבע רשם מאגרי מידע שערך רישום של משתמשי הנתונים ולשכות השירות. נשוא הנתונים מחזיק בזכות חוקית לקבלת המידע המוחזק אודותיו. חבר שופטים (Tribunal) יסייע בפתרון חילוקי הדעות שיתעוררו בין המשתמשים בנתונים לבין רשם מאגרי המידע. אזרחים שיסבלו ממידע לא מדויק, או מנתונים שאינם מוגנים כנדרש, יוכלו לתבוע פיצוי מהמחזיקים בנתונים אלה.

9.5.1 החוק להגנת נתונים משנת 1984

כמו כל חוק, גם החוק להגנת נתונים הוא מסובך, וכדי להבין את השלכותיו, יש לנתח אותו לפי מאפיינים דומים בחוקים אחרים. אין זה החוק האנגלי הראשון שמעניק לאזרח זכות לבדוק ולקרוא תיגר על המידע המוחזק אודותיו על ידי זולתו. חוק האשראי לצרכן (The Consumer Credit Act, 1974) מעניק לאזרחים זכויות דומות ביחס לחברות האשראי.

לחוק זה יש 43 סעיפים, המקובצים בחמישה פרקים:

(1) הקדמה
(2) רישום ופיקוח על משתמשי הנתונים ולשכות שירות
(3) זכויות נשואי הנתונים
(4) חריגים
(5) כללי

בנוסף לחמשת הפרקים, ישנם ארבעה נספחים שמהווים הסבר לעקרונות של הגנת הנתונים, לתפקידי רשם מאגרי הנתונים וחבר השופטים, להליכי הערעור ולמחזיקים בסמכויות לרישום ולביקורת. שמונה העקרונות להגנת נתונים, הנמצאים בנספח מספר 1, מוצגים בטבלה 9.6. בעת רישום מאגר מידע יימסרו הפרטים שמובאים בטבלה 9.7.

אם בקשה לרישום מאגר נתונים נדחית, או אם הרישום בוטל, רשאי המשתמש בנתונים לערער בפני חבר שופטים. הרשם מחזיק בסמכויות להבטיח שהשימוש במידע אישי ייעשה בהתאם לעקרונות הגנת הנתונים. אדם שיעבור על החוק צפוי לקנס והנתונים הקשורים למקרה יימחקו. לפי החוק, העבירות הפליליות היחידות הן אלו שקשורות לרישום, כמו למשל, אי רישומו של מאגר, או אי עמידה בתנאים. בכל הנסיבות האחרות, על נשוא הנתונים להגיש תביעה אזרחית.

טבלה 9.6 עקרונות להגנת נתונים לפי נספח מס' 1 מהחוק האנגלי להגנת נתונים (1984)

מידע אישי המוחזק על ידי משתמשי הנתונים
1. מידע אישי יושג ויעובד בצורה הוגנת ולפי החוק. 2. הנתונים יוחזקו וישמשו למטרות ייעודיות בלבד. 3. מידע לא ייחשף ולא ייעשה בו שימוש כלשהו, אלא למטרות שלשלמן הוא נאסף. 4. המידע המוחזק למטרה כלשהי יהיה בכמות מספקת, ולא מעבר לכך. 5. המידע יהיה מדויק ובמקרה הצורך, מעודכן. 6. מידע לא יישמר לתקופה הארוכה מזו שנחוצה למטרה שלשמה נאסף.
זכויות נשוא הנתונים
7. נשוא הנתונים מחזיק בזכויות הבאות: * גישה אל הנתונים האישיים שמתייחסים אליו. * גישה לנתונים אלה בפרקי זמן סבירים וללא עיכוב. * תיקון ו/או מחיקה של נתונים, לפי הצורך.
אמצעי הגנה
8. על משתמשי מחשב ולשכות שירות להתקין אמצעים מתאימים להגנת הנתונים מפני גישה ללא הרשאה, חשיפה, שינוי, הרס, או אובדן בשגגה.

טבלה 9.7 פרטי הרישום

1. שם וכתובת של המשתמש במחשב, או לשכת השירות.
2. תיאור של הנתונים המוחזקים ושל המטרה שלשמה הם מוחזקים.
3. המקורות שמהם נאספים הנתונים.
4. זהות האנשים שבפניהם ייחשפו הנתונים על ידי המחזיק בהם.
5. שמות של מדינות זרות שאליהן יועברו הנתונים.
6. שם וכתובת של אדם שיטפל בכל הבקשות של נשוא הנתונים

9.5.2 חריגים

החוק מתייחס רק למידע שמעובד באופן אוטומטי ולכן, מידע המטופל באופן ידני אינו כפוף להוראות החוק. בנוסף, סוגים מסוימים של יישומי מחשב פטורים באופן חלקי, או מלא, מדרישות החוק. אפשר לסווג חריגים אלה לשתי קבוצות עיקריות:

(1) יישומים שאינם מהווים איום לנשואי הנתונים. לדוגמה, מידע אישי המוחזק לצרכים ביתיים.

(2) יישומים קריטיים לאינטרסים של המדינה, או לרשויות הציבוריות. לדוגמה, מידע המתייחס לפשעים או למיסים.

החריגים בנושא זה יכולים להיות מהסוגים הבאים:

(1) זכויות הגישה של נשוא הנתונים, כמפורט בטבלה 9.8, להוציא את הנושאים הבאים:
 (א) מידע המשמש לגילוי פשעים.
 (ב) מידע הקשור לבריאות פיסית ונפשית.
 (ג) מידע הקשור למיסים.
 (ד) מידע הקשור לעבודה סוציאלית.

(2) כללי אי-חשיפה. במצבים מסוימים, כמתואר בטבלה 9.9, אפשר לחשוף נתונים בפני אדם שאינו נמצא בפרטי הרישום של המאגר.

(3) כל הפרקים של החוק, המפורטים בטבלה 9.10 וכוללים מידע המוחזק למטרות של בטחון, אינם כפופים לחלוטין לחוק זה.

טבלה 9.8 נסיבות שבהן אין לנשוא הנתונים זכות לראות את הנתונים

1. נתונים המשמשים לאכיפת החוק: מידע המוחזק למטרות אכיפת חוק וגביית מס הכנסה, שגישה אליו תפגע במטרות אלה. 2. מידע המוחזק על ידי גופים מסויימים לצורך הסדרה ואספקה של שירותים פיננסיים. 3. מידע שהחוק מאפשר לו זכות יתר זו, או מידע הקשור למינוי שופטים. 4. מידע המשמש לצרכים סטטיסטיים או לצרכי מחקר: נתונים אלה לא ישמשו מטרות אחרות ויוצגו ללא פרטים מזהים של נשואי המחקר. 5. נתונים לגיבוי: נתונים אלה נועדו למקרה שהמידע שבמחשב ייהרס או ייפגע בצורה אחרת. 6. מידע הקשור לעבודה סוציאלית ולבריאות פיסית ונפשית: ההכרעה הסופית אם לאפשר כניסה לנתונים אלה נתונה למזכיר המדינה.

טבלה 9.9 נסיבות שבהן ניתן לחשוף מידע בפני אדם ששמו אינו נמצא בטפסי הרישום

החשיפה מתייחסת למקרים הבאים: 1. אכיפת החוק 2. גביית מס הכנסה 3. בטחון לאומי 4. הליכים משפטיים 5. מניעת נזק בריאותי 6. בהסכמת נשוא הנתונים

בטבלה 9.10 מפורטים סוגי מידע מסוימים, שהשימוש בהם משמעותי לתעשיית עיבוד הנתונים, כמו למשל, מידע המוחזק לצרכים של דיוור ישיר שמכיל שמות וכתובות, המוחזקים על פי אישור מנשוא הנתונים וכפופים למגבלות חשיפה. התנאים לכל פטור הם קריטיים, אך התנאים החמורים ביותר קשורים למידע המוחזק לצורכי משכורות וגמלאות בלבד, או לצרכים חשבונאיים ותחזיות פיננסיות וניהוליות בלבד.

טבלה 9.10 מידע הפטור לחלוטין מחוק הגנת הנתונים משנת 1984

סוגי המידע הבאים פטורים לחלוטין מכפיפות לחוק. בחלק מהם, הפטור מותנה במילוי תנאים מסוימים. 1. מידע המוחזק לצרכי בטחון לאומי. 2. מידע המוחזק רק לצרכי משכורות וגמלאות. 3. מידע המוחזק רק למטרות חשבונאיות. 4. מידע המוחזק רק לצורך הכנת מסמכים. 5. מידע המוחזק רק לצרכים ביתיים. 6. מידע המוחזק לצרכים של דיוור ישיר.

אם המשתמש בנתונים טוען לפטור מכפיפות לחוק, חשוב מאוד שיהיה מודע לכל הכללים, כדי שיוכל להוכיח בכל זמן שהוא פועל לפיהם.

9.5.3 יישום החוק

החוק נכנס לתוקף בספטמבר 1985. כדי לסייע לארגונים ביישומו, פרסם הרשם סדרה של קווים מנחים, שחולקו בפברואר, 1985, למשתמשי מחשב. בפרסום זה הוצע למשתמשים לבצע את הפעולות הבאות:

* למנות קצין אבטחת מידע.
* להודיע לעובדים על שינויים בנוהליי האבטחה.
* לבצע רישום של כל סוגי הנתונים.
* לברר האם ניתן לטעון לפטור.

יש לסווג את הנתונים לרישום לפי הקטגוריות הבאות:

* נתונים אישיים המוחזקים במערכות ידניות.
* נתונים אישיים המוחזקים בקבצי מחשב.
* נתונים לא אישיים.
* רמות רגישות.

בטווח הקצר, חשוב לרשום מידע אישי המוחזק במערכות ידניות, כי הוא יוכל לשמש בסיס לפטור מהחוק. אך בטווח הארוך, מידע זה יהיה חשוב יותר, מכיון שסביר להניח שנתונים המוחזקים כיום במערכות ידניות יועברו בעתיד לקבצי מחשב.

9.5.4 העלות והביקורת

בכל השלבים שעבר החוק עד לאישורו, נדונו ההשלכות הכספיות שלו. ההוצאות עבור הרשם ומשרדו ועבור חבר השופטים הוערכו ב-650 אלף ליש"ט לשנה. המימון צפוי היה להגיע מדמי הרישום. ההוצאה של משרדי הממשלה לפיתוח חומרה ותוכנה הוערכה ב-5.5 מיליון ליש"ט לשנתיים הראשונות. קשה מאוד להעריך את עלות הזכות של נשואי הנתונים לראות את הנתונים המתייחסים אליהם. הוערך, שאם אחוז המבקשים יהיה 0.1 מכלל בעלי הזכות, יגיעו הוצאות התפעול למיליון ליש"ט לשנה. הוצאות היישום והתפעול לרשויות מקומיות הוערכו ב-10 מיליון ליש"ט לשנה ולגופים ציבוריים - ב- 13 מיליון ליש"ט לשנה. ההנחה היתה שחברות פרטיות יספגו את הוצאות ההתקנה והתפעול. מהניסיון שנצבר במדינות אירופאיות אחרות, אפשר לראות שמספר הבקשות של נשוא הנתונים לראות את נתוניו נמוך מאוד, וכך גם מספר התביעות לפיצוי, כתוצאה מנזק שנגרם על ידי מידע לא מדויק.

אפשר להסיק (וונג, 1984) שההוצאות שנגרמו לארגונים בגלל החוק היו גבוהות לעומת התועלת שהוגשה. דיעה אחרת על החוק (גוסטין, 1984) גורסת "שלמרות שהיוזמה מבורכת, אין היא יעילה בשמירה על רשומות של מידע אישי. היא קשה לתפעול ואינה עומדת בדרישות שותפינו לשוק האירופאי". הביקורת נובעת מכמה סיבות:

* הכישלון לכסות רשומות ידניות.
* החוק אינו כולל כללי שימוש, ולכן הפרשנות בנושא זה נשארת בידי השופטים בבתי המשפט האזרחיים.
* קיימת דאגה לגבי תפקיד "כלב השמירה" שממלא משרד הפנים, שעלול לעמוד בסתירה למחויבותו כלפי משרדי ממשלה אחרים המחזיקים במידע רגיש.

9.6 סיכום

כיום אזרחים נספרים, נמצאים תחת פיקוח, נרשמים ונשאלים על ידי ארגונים ממשלתיים ופרטיים יותר מאשר בעבר (נורבק, 1981). מאגר גדול זה של מידע אישי גורם לסכנה, הגדולה יותר מתמיד, שמידע אישי סודי יפול לידיים הלא נכונות. לכן, התחיקה בנושא הגנת נתונים צריכה לספק אמצעי הגנה שיענו על צרכי האזרחים, אך לא יפריעו לזרימת המידע אל ארגונים ומהם.

בבריטניה קיימת הסכמה רחבה בעניין הצורך בחוקים יעילים להגנת נתונים. למרבה הצער, הנושא מסובך ולכן התעורר ויכוח ציבורי חסר תכלית על אופיו של החוק. התוצאה הסופית הושפעה

מגורמים טכניים, מסחריים ומאלה הקשורים בזכויות האדם. גם הניסיון של מדינות אחרות השפיע על ההכרעה. לדוגמה, בצרפת דווח שבתחילת 1982 רק חמישית מכל הארגונים שהיו צריכים להרשם, אכן נרשמו. ובכל זאת, הלחצים הגוברים שהתחילו בשנות והמשיכו בשנות ה-80 הביאו, בסופו של דבר, לחקיקה ב-1984.

החקיקה הקיימת משתנה במידה רבה בין מדינה למדינה. אין זה טוב, מכיוון שאם נתונים מועברים ממדינה עם חוקים מוגדרים ונוקשים למדינה שאמצעי ההגנה בה אינם מספיקים, הגנתם מתערערת. למרות שהלחץ הבינלאומי לתקנות משותפות התגבר, המצב באירופה לא השתנה, כלומר, יש תקנות שונות בכל מדינה. העובדה שבמדינות רבות חוקקו כבר חוקים להגנת נתונים והשיתוף והשיתוף הקיים של מועצת אירופה בענין זה, מבטיחים שהבעיה תפתר באופן יסודי באירופה בעתיד הקרוב.

התחיקה בנושא הפרטיות משפיעה על התכנון והתפעול של מערכות מידע. הרישום של מאגרי הנתונים יהיה חלק בלתי נפרד מהפיתוח. מתכנני מערכות יידרשו לספק רמה חסרת תקדים של אבטחה, ואילו משתמשי הקצה יבקשו מהמתכננים לייעץ להם על הדרך שבה יש לבנות את המערכת שלהם, כדי שתעמוד בדרישות החוק. יהיה צורך לאשר מספר גדול של מערכות קיימות וחדשות ויש לצפות לעלייה משמעותית בהוצאות.

בארצות הברית נעשו ניסיונות להעריך את המשמעות הכספית של יישום בקרות הפרטיות (גולדשטיין, 1976). ההשפעות של תחיקה כזו אינן מוגבלות רק לפיתוח, אלא גם לתפעול של מערכות מידע. יש לתכנן אמצעים שיאפשרו לבדוק אם המערכות פועלות במסגרת החוק. אחת הדרכים להשיג זאת היא דרך ביקורת פרטיות (rivacy Paudit, דלויט ואחרים, 1982), שאפשר לבצעה בו זמנית עם ביקורת פיננסית. הטענה שהמחיר הגבוה של הגנת נתונים הוא בעייה שאינה ניתנת לפתרון אינה רלוונטית, מכיון שנושא זה קשור לזכויות האדם ונוגע באופן ישיר לאיכות חיינו.

שאלות

9.1 "אי היעילות והמגבלות הטבעיות של מערכות ידניות הן ההגנה על הפרטיות שלנו." מהי דעתך?

9.2 קשה לתכנן מערכות מידע שיעמדו בדרישות של חוקי הפרטיות. הסבר, בכל זאת, את מאפייני התכנון הדרושים כדי לספק את הדברים הבאים:
(א) זכות הפרט לדעת אילו נתונים מוחזקים בקשר אליו.
(ב) זכות הפרט לבדוק את הרשומה הנוגעת לו.
(ג) החובה להשתמש במידע למטרות המוצהרות בלבד.

9.3 חברה הרוצה לעמוד בדרישות החוק להגנת נתונים תספוג הוצאות התקנה וכתוצאה מכך, הוצאות תפעול נוספות. הסבר מהם המרכיבים הבסיסיים של הוצאות אלו.

9.4 הניסיון האירופאי מלמד שמספרם של המבקשים לראות את הנתונים שנשמרים אודותיהם נמוך, כמספר התביעות לפיצוי בגין נתונים לא מדויקים. מצב זה קיים גם בישראל. מהי דעתך על ההצהרה: "ההוצאות המשמעותיות שארגונים חייבים לספוג כדי לעמוד בכל דרישות החוק, אינן תואמות לתועלת" (וונג).

9.5 בבעלותו של ארגון מערכת מידע המכילה נתונים אישיים הנוגעים לאנשים מחוץ לארגון. מערכת זו היא ידנית. מהם לדעתך הגורמים שישפיעו על החלטה בעד או נגד המעבר למערכות המבוססות על מחשב.



אותם משרתים והם גם האיומים על המערכת

פרק 10

הגנה על התוכנה

הפצת תוכנות מחשבים פירטיות היא פשע נפוץ. להגנה על תוכנה יש משמעות לבעלים, למשתמשים, למפתחי התוכנה ולציבור הרחב. אפשר להגן על תוכנות בעזרת אמצעים משפטיים וטכניים. שלושה חוקים מציעים כיום הגנה פוטנציאלית על תוכנות: חוק הפטנטים, חוק זכויות יוצרים וחוק סודות מסחריים. הגנה טובה תושג על ידי שילוב של אמצעי הרתעה טכניים ומשפטיים.

10.1 העילה להגנה

הפירטיות היא הפצה או העתקה לא חוקית של תוכנות, השגת תוכנות ששייכות לאחרים, לעתים גם עריכת שינויים והפקת רווח כספי מהשימוש בתוכנות, או ממכירתן.

באופן מסורתי, מנסה תעשיית המחשבים ליצור תוכנה שתהיה ניידת וקלה לשימוש. שיטה זו כוללת שימוש בגירסאות סטנדרטיות של מערכת ההפעלה, מהדרים ומפרשים (interpreters). תוכנה ניידת מקלה על פירטיות. הדרישה לניידות של תוכנות מנוגדת לצורך בהגנה עליה.

הפצה פירטית של תוכנות למחשבים גדולים לא היוותה מעולם בעיה. הסיבה המרכזית לכך היא שהמחשבים מוחזקים על ידי ארגונים שאינם יכולים לעסוק בפירטיות ויש להם תקציב לרכישת תוכנה רשמית המלווה בהדרכה, עדכונים ותמיכה טכנית. תמיכת הספק היא חלק אינטגרלי וחיוני של התוכנה. המאפיינים של שוק המחשבים האישיים שונים. למשתמשי המחשב אין תקציבים גדולים. לעתים קרובות, המחשבים האישיים הם חלק מעסקים קטנים ונחשבים כמוצרי צריכה. תעשיית התוכנה למחשבים אישיים נפגעת קשות על ידי פירטיות. לדוגמה, מניחים שעל כל חבילת WORDSTAR מקורית, שנמכרה בבריטניה, קיימים שלושה העתקים פירטיים. כרבע מכלל ספקי התוכנה למחשבים אישיים סובלים באופן משמעותי מפירטיות.

ההגנה על תוכנה מפני פירטיות צריכה להיות מעניינם של הבעלים, המשתמשים, יוצרי התוכנה והציבור הרחב (שטרן, 1982). טבלה 10.1 מראה שהקבוצות הללו מתייחסות באופן שונה, ולעתים

אף מנוגד, להגנה על תוכנות. ניגוד אינטרסים, בשילוב עם בעיות משפטיות, עשוי להסביר מדוע תופעת ההפצה הפירטית עדיין לא נפתרה.

טבלה 10.1 קבוצות בעלות עניין בהגנת תוכנה

הקבוצה	האינטרס של הקבוצה	יעדי ההגנה
בעלי התוכנה	הגנה על השקעה כספית	הגנה משפטית מקסימלית
מנתחי מערכות ומתכנתים	הכרה רחבה ביוצרי התוכנה (לכן הגנה רצויה, אך אנשי מחשב רוצים, בדרך כלל, גישה חופשית לרעיונות חדשים)	הגנה טובה מזו הקיימת היום
משתמשים (לדוגמה, חברות)	תוכנה זולה ככל האפשר	ללא הגנה בטווח הקצר (בטווח הארוך, תקטן כמות התוכנות החדשות ומחירן למשתמש יגדל)
הציבור הרחב	פיזור ידע ומניעת העתקה ללא צורך (המתאזנים עם גמול נאות לתמורה אמיתית)	הגנה מינימלית

10.2 שיטות להגנה על תוכנה

בנוסף לאמצעי הגנה טכניים, קיימים שלושה תחומים בחוק שנוגעים לפטנטים, לזכויות יוצרים ולסודות מסחריים, אשר מאפשרים הגנה לתוכנה (מוהר, 1975; פרנז', 1981; גרהם, 1984). כל אחד מתחומים אלה מציב הגבלות על המפתח, ומציג קושי בהגדרה של תוכנת מחשב.

בהמשך, נסקור את שלושה התחומים שהונהגו בחוק הבריטי. נסקור את הניסיון שהצטבר בארצות הברית, שבה השימוש במחשבים נפוץ יותר ונציג כמה תביעות משפטיות בנושא. סקירה של המבנה המשפטי בבריטניה, המוצגת בטבלה 10.2, מראה את המבנה ואת הגישות השונות לזכויות יוצרים, פטנטים וסודות מסחריים. נראה

את האופן שבו הם התפתחו עד היום, במטרה לספק הגנה נאותה למצבים מקובלים, שאינם קשורים במחשוב, וניווכח שההתייחסות שלהם לתוכנה אינה מספקת.

10.3 חוק זכויות יוצרים

מבחינה היסטורית, המוציאים לאור ובתי הדפוס, ולא הסופרים, היו אלה שביקשו בבריטניה הגנה על זכויות יוצרים. חוקים שונים בנושא זה נחקקו במהלך 200 השנים האחרונות והאחרון שבהם הוא חוק זכויות יוצרים מ-1956.

חלק מס. 1 של חוק זה מתייחס להגנה על זכויות יוצרים בעבודה ספרותית (כלומר, מלים כתובות או מודפסות), והוא שיכול להגן גם על תוכנה. חלק מס. 2 מתייחס לזכויות מפיקי סרטים, הפקות קוליות והקלטות אחרות. הביקורת על חוק זהמכוונת לכך שהוא אינו מבטא עקרונות בסיסיים (קורניש, 1981) ואינו כולל התייחסות למחשבים. ב-1977, פורסם בדוח רשמי על צורך דחוף לתיקון חוק זכויות יוצרים, כדי שיכיל את הטכנולוגיות החדשות (Cmnd 6732, 1977).

טבלה 10.2 משך ההגנה המקובל על ידי החוקים הקיימים והתחומים שעליהם הם מגינים

החוק	משך ההגנה	מספר הקבוצות המושפעות	התחומים שעליהם מגן החוק
זכויות יוצרים	חיי הסופר + 50 שנה	אינסופי	עבודות ספרותיות
פטנטים	20 שנה	אינסופי	רומן, המצאות תעשיתיות
סודות מסחריים	עד שהסוד הופך לנחלת הכלל	קבוצה קטנה	1. רעיונות. 2. ישים גם לתוכניות הנמצאות מעבר לשלב הרעיון.
זכויות על פי חוזה	לתקופה שהוסכמה בין הצדדים	החותמים	3. כל שיטה שמוכרת למעט מאוד אנשים.

חוק זכויות יוצרים מגדיר יצירה ספרותית "כל יצירה שהושקעו בה כישרון, עבודה וכושר שיפוט". בנוסף, עבודה ספרותית חייבת להיות מקורית. מקוריות מתייחסת לסופר ולא לרעיונות המובעים ביצירתו. זוהי הגדרה צרה, אך יש לה כמה יתרונות:

(1) מקוריות היא עניין אובייקטיבי ולא סובייקטיבי ולכן, בתי המשפט יכולים להכריע בקלות יחסית אם להגן, או לא להגן, על יצירה.
(2) אפשר להגן על מגוון רחב של יצירות ספרותיות.

המעמד של חוק זכויות יוצרים לגבי תוכנה אינו ברור, בגלל מספר קטן של תביעות משפטיות. לאחרונה החלו חברות גדולות למשחקי וידאו לטעון שחברות אחרות פגעו בזכויות היוצרים של משחקי הוידאו שלהן, כשהעתיקו ומכרו את עותקיהם. ברבים מהמקרים האלה מושגת פשרה לפני התערבות בית המשפט ועלול לעבור זמן רב עד שבתי המשפט בבריטניה יחליטו אם להגן על תוכניות מחשב באמצעות חוק זכויות יוצרים, אלא אם חקיקה חדשה תזרז את מהלך העניינים. דוח הבנקים (Banks Report) ודוח וויטפורד (Whitford Report) תמכו בהענקת הגנה של חוק זכויות יוצרים לתוכניות מחשב. וועדת וויטפורד גם סייעה בהבהרת מעמד התוכנה כאשר קבעה שכתיבה יכולה להתייחס לשיטות אחרות של רישום מידע, בכללן אחסון על דיסקים או על סרטים.

בארה"ב קיימים שני סוגים שונים של זכויות יוצרים:

(1) ברמה הפדרלית, ניתן לטעון זכות יוצרים על עבודה שפורסמה, סומנה בסימן המוסכם (C) ונרשמה במשרד לזכויות יוצרים.
(2) ברמת המדינה, אפשר לטעון לזכות יוצרים על עבודה מיד לאחר שנכתבה, אפילו לפני שפורסמה ברבים.

אפשר לטעון לזכות יוצרים לגבי תוכנות מחשב מאז 1964, כאשר המשרד לזכויות יוצרים החליט להתייחס לתוכניות כאל ספרים, עם סייג הקובע שהתוכניות צריכות להיות ניתנות לקריאה על ידי בני אדם. בין השנים 1964 ל-1978 נרשמו רק אלף תוכניות מתוך כשלושה מיליון. לא נרשמה אף לא תביעה משפטית אחת.

בינואר 1978 נכנס לתוקפו חוק זכויות יוצרים חדש שמגן באופן מפורש על טכנולוגיות חדשות. החוק מאפשר לכותב לבצע תרגומים לשפות ולדיאלקטים אחרים. לאחרונה התקבלו כמה החלטות סותרות של בתי משפט פדרליים, המעידות שהחוק החדש אינו מפורש באופן מספק לגבי תוכניות בקושחה (ROM) ולגבי צורות אחרות של תוכנה (מקלנינג, 1983).

אחד המקרים מתייחס לקושחה שנבנתה במיוחד כדי להיות חלק אינטגרלי של משחק שחמט (שטרן, 1982). התובע טען שהקושחה נגנבה על ידי פירוק (unload) שלה על ידי הנאשם, שהעביר באופן זה את הקוד לקושחה אחרת, ששימשה בסיס להעתקות. בית המשפט קבע שלא היתה הפרה של זכות יוצרים, בנימוק שבניינים הנבנים על פי תוכניות ארכיטקטוניות אינם נחשבים להעתקים. משמעות החלטה זו היא שתוכנית ארכיטקטונית מוגנת על פי חוק זכויות יוצרים אך לא הבניין עצמו. בדומה, תוכנית המקור מוגנת כיצירה, אך תוכנית היעד (object program) היא כלי מכני, כמו הבניין, ולכן אינה מוגנת על ידי חוק זכויות יוצרים.

במקרה אחר, הנוגע למשחק וידאו המופעל באמצעות מטבעות, נקבע שאין זה חוקי להפיק עותק של תוכנית הנמצאת בתוך קושחה. ההחלטה התבססה באופן חלקי על העובדה שהנאשם גרם להצגת התוכנית על יחידת תצוגה והעתיק אותה כדי ליצור על פיה קושחה אחרת. היו מספר תיקונים לחוק בשנות ה-80, אך זכויות המחבר לקושחה ולצורות אחרות של תוכנה, עדיין מוטלות בספק. למרבה המזל, תוכניות המקור מוגנות.

10.4 חוק הפטנטים

לחוק הפטנטים באנגליה היסטוריה ארוכה המתחילה בהתרחבות המסחר, שחלה במחצית הראשונה של המאה ה-15. לכן התפתח נוהל מוגדר היטב, שבו מתקיים חוזה בין הממציא לבין המדינה. הממציא מספק מידע על ההמצאה והמידע הופך לנחלת הציבור. בתמורה, מקבל הממציא בלעדיות על השימוש בהמצאה. בטבלה 10.2 נוכל לראות שהבלעדיות נשמרת שנים רבות. מטרות הפטנט:

(1) ברמת הפרט, לעודד ממציאים להמציא ולעודד אותם להשתמש ברעיונות שלהם בשוק החופשי, ללא חשש מגניבות.

(2) ברמת המדינה, להקטין את כמות הכפילויות ולתרום לשגשוג ולקידמה של אזרחיה.

למרות שחוק הפטנטים אינו מהווה הגנה מספקת לתוכנה, אין הוכחות שממציאים נמנעו מפיתוח תוכנות במהלך העשור האחרון. עובדה זו סותרת את התיאוריה שללא הגנת חוק הפטנטים תהיה נסיגה במספר המוצרים החדשים (טפר, 1982).

לחוק הפטנטים באנגליה כמה דרישות:

(1) מקוריות - אין אפשרות לרשום פטנט על מוצר (אובייקט) שמשקף את הטכנולוגיה הנוכחית.

(2) שלב ההמצאה - ההמצאה לא תהיה מובנת מאליה על ידי מומחים בתחום.
(3) יישום תעשייתי - ההמצאה צריכה להיות כזו שיהיו לה דרישה או צורך ליישום בתעשייה.
(4) חשיפת ההמצאה - מפרט הפטנט צריך להיות ברור ושלם, כדי שבעל מקצוע אחר יוכל לבנות את המוצר
(5) אפשרות רישום כפטנט - לפי החוק הקיים משנת 1977, לא יירשמו הדברים הבאים כפטנט: גילויים (discoveries), תיאוריות מדעיות ונוסחאות מתמטיות. החוק מציין במפורש שניתן לרשום תוכניות מחשב כפטנט.

משרד הפטנטים הבריטי הוציא בשנת 1969 מסמך המצהיר שלא ניתן לרשום תוכניות מחשב כפטנט. מאוחר יותר, המליצה ועדת הבנקים שלא לאפשר לרשום כפטנט תוכניות ששלב ההמצאה שלהן נמצא בתוכנית עצמה. ההמלצה התייחסה לדוגמה של מפעל פלדה המבוקר על ידי מחשב שיוכל להרשם כפטנט רק אם החידוש אינו בפרטי התוכנית (Cmnd 4407, 1970). היתה זו הפעם הראשונה שהחוק הבריטי התייחס במפורש לתוכניות מחשב.

תוכניות מחשב אינן נכללות בחוק הפטנטים הנוכחי משנת 1977 הנהוג בבריטניה. הדבר נעשה בתיאום עם וועדת התחיקה האירופאית לנושאי פטנטים. למרות זאת, בקשה לרישום פטנט הקשור לתוכנית מחשב תוכל להתקבל, אם התוכנית היא חלק מתהליך תעשייתי. לפי חוק זה,מספר הפניות לרישום תוכניות מחשב, כפטנטים יהיה קטן ויוגבל מאוד רישומם של פטנטים הכוללים תוכניות מחשב.

המסלול שעבר חוק הפטנטים בארצות הברית היה עקלקל, אך שונה מהמקרה הבריטי. ב-1968 החליט משרד הפטנטים שתוכניות לא יהיו כשירות לרישום, אך ב-1969 הוחלט שכל בקשה תיבדק לגופה. ב-1971 קיבלו חברי ה-Court of Customs-, וועדת הערר של משרד הפטנטים - החלטה חשובה במיוחד. הם החליטו לרשום כפטנט תוכנית שממלאת אחר התנאים הבאים:

(1) התוכנית ממירה ייצוג בינארי של מספרים עשרוניים למספרים עשרוניים טהורים.
(2) הציוד שבו אמורה התוכנית להשתמש אינו מפורש.

אין זה מפתיע שבית המשפט העליון ביטל החלטה זו לאחר זמן קצר. מאוחר יותר, התקבלה הסכמה בין בית המשפט העליון לבין משרד הפטנטים. ב-1978 תמך בית המשפט העליון בעמדת משרד הפטנטים, המנוגדת לזו של בית המשפט פדרלי, וסרב לרשום כפטנט תוכנית המחשבת ערכי גבול להפעלת אזעקה בתהליך כימי תעשייתי. נקבע שהתוכנית אינה חדשנית בגישתה. בהחלטה נאמר שבית המשפט

צריך לדאוג לכך שלא יהיה מונופול על עקרונות מופשטים, מכיוון שהם כלי עבודה חיוני בפיתוח הטכנולוגיה. ב-1981 קבע בית המשפט העליון החלטה מנוגדת, ואיפשר לרשום כפטנט תהליך תעשייתי המשלב תוכנית מחשב (הייהרסט, 1982).

מקרה מעניין אחר הוא זה של Valport, שההתדיינות המשפטית בו נמשכה כעשר שנים. ב-1982 נרשמה החבילה הפיננסית Valport כפטנט. הרישום התייחס לשיטה לפעלת מחשב שבו רצה מערכת Valport ולא "סתם" תוכנית פשוטה (אנטיקנאפ, 1982). Valport מחשבת ערכים ריאליים של תיקי מניות. היא מכפילה כל מניה במחיר השוק האחרון שלה, כדי לקבל את ערכה הריאלי. Valport אינה משווקת כחבילה אלא כשירות בשיתוף זמן עם בסיס נתונים, המכיל למעלה מ-60,000 מניות. אפשר להפיק מבסיס הנתונים יותר מעשרה דוחות שונים, בשירות שניתן באמצעות מסוף ומודם חיוג. הפטנט מתייחס למערכת הכוללת של הערכת תיקי מניות, המספקת שירות בו-זמני למשתמשים רבים, הפונים לבסיס נתונים שמתעדכן מדי יום. האם בעתיד יוכלו חבילות אחרות להרשם כפטנט?

ההחלטות הסותרות מקשות על מלאכתם של התובעים והבוחנים. טפר מציע שדיעות על חוקיות הרישום יתבססו על פירוש הודעות רשמיות של בית המשפט העליון ועל ניתוח החלטות ספציפיות. למרות זאת, נראה שבקשות לפטנט לא יתקבלו אם מדובר באלגוריתם, אך יצליחו להתקבל אם התוכנית תהווה חלק מההמצאה היוצרת תהליך תעשייתי. למרות ההתפתחויות השונות, אין חוק הפטנטים הנוכחי בארצות הברית שונה בפועל מהחוק הבריטי.

10.5 סודות מסחריים ושמירת סודיות

יתרונו של החוק המתייחס לסודות מסחריים ושמירת סודיות הוא בכך שאפשר להתאימו בקלות לטכנולוגיות ולמצבים חדשים. התפתחות החוק היתה מקרית במידת מסוימת. חוק זה, המקיף יותר מחוק הפטנטים וחוק זכויות יוצרים, יכול להגן על תוכניות מחשב. לדוגמה, אפשר למנוע ממנתחי מערכות וממתכנתים, באמצעות סעיף חוזי, מלחשוף את התוכנה לגורמים אחרים בתקופת עבודתם בארגון ולאחריה. אפשר גם להגן באמצעות חוק זה על תיעוד, כמו נוהלי עבודה ותרשימי זרימה של נתונים.

החוק לסודות מסחריים ולשמירת סודיות מוגבל באופן טבעי לדברים סודיים או חסויים. בבריטניה מוגנות תוכניות מחשב על פי חוק זה, אך לא דווחו מקרים על השימוש בו.

בארצות הברית, החוק הוא הדרך הנפוצה ביותר להגנה משפטית. בכך משתקפת אזלת ידם של חוק זכויות יוצרים וחוק הפטנטים.

חוק הסודות המסחריים ושמירת הסודיות שונה מחוק הפטנטים ומחוק זכויות יוצרים, בכך שאינו פדרלי. אנשים וארגונים יכולים לקשור חוזים ביניהם, אך קושי מתעורר כאשר מעורב גורם שלישי. חוזה בין A ל-B אינו קושר צד שלישי X, אלא אם X מעודד ביודעין את B להפר את הסכם הסודיות עם A. במקרים כאלה X יכול לקנות מ-B מחשב המכיל קושחה שנבנתה ונוצרה על ידי A ולפרוק (unload) את הקושחה, ללא חשש מעונש. גם אם מכירת הציוד מ-B ל-X מהווה הפרת החוזה בין A ל-B, אין ל-A כל עילה לתביעה נגד X.

10.6 שיתוף פעולה בינלאומי והרפורמה בזכויות יוצרים

החוקים שנדונו לעיל פותחו למטרות שונות, אך לא לתוכניות מחשב. חוק הפטנטים מתאים למוצרים ממשיים, אך אינו מתאים למידע. חוק זכויות יוצרים מתאים להגנה מפני העתקה של צירופי מילים, שרטוטים ולכאורה גם תוכנה, אך יעילותו מוגבלת מאוד בהגנה מפני שימוש לא מורשה בתוכניות. היקף ההגנה שמספקים חוק סודות מסחריים וחוקי החוזים לא ברור, במיוחד כאשר הצדדים אינם נכללים בחוזה.

אי שביעות רצון כללית מהחוק עוררה דרישה לחקיקת חוק חדש, שיענה על הבעיות המיוחדות של תוכנה. הוצעו שינויים מגוונים, החל מתיקונים קוסמטיים בחוק הקיים ועד חוק מיוחד בנושא תוכנה. הוצעה גם שיטה לשימוש נרחב בחוק הפטנטים, אך העלות הגבוהה הצפויה עלולה היתה להרתיע תובעים, מלבד הרציניים ביותר, ולהפלות לטובה את הארגונים העשירים. מסיבה זו, השיטה אינה מקובלת.

הצעה אחרת היא רישום התוכנה. הבעלים רושם עותק של התוכנה ותיאור התפישות של הפיתוח שלה. הרשם מפרסם מייד את תיאור התפישות, אך התוכנה נותרת חסויה במשך עשר שנים. העלות של שיטה זו היא נומינלית, מכיוון שנוהל זה אינו מחייב בדיקה של הרשם, או שנערכת בדיקה מינימאלית. שיטה זו, שהוצעה על ידי חברת יבמ ב-1968, נועדה לשמש תוכניות גדולות, שחוק הפטנטים חל עליהן ממילא. הרישום יכול להגן מפני העתקה לא חוקית, אך אפשר לפתח תוכנית דומה לפי התפישות שפורסמו ברבים. נקודת התורפה בהצעה זו היא שקשה מאוד להוכיח אם תוכנה פותחה באופן עצמאי או הועתקה.

הצעה נוספת קבעה שהשיטה הטובה ביותר להגנה על תוכנות היא להקפיד שהחוקים הנוגעים לזכויות יוצרים ברחבי העולם יהיו אחידים. קשה להגיע לכך אפילו בתחומה של יבשת אירופה. לדוגמה, תקופת ההגנה משתנה ממדינה למדינה ותוכנה מסוימת

יכולה להיות מוגנת במדינה אחת כאשר פג תוקף הגנתה בשאר המדינות, כמתואר בטבלה 10.3 (הערת המתרגם: ייתכן שהמצב ישתנה לאחר 1992).

טבלה 10.3 משך החלת זכות יוצרים במדינות אירופה השונות

המדינה	משך ההגנה: חיי הכותב בצירוף הזמן המוצג
גרמניה ואוסטריה	70 שנה
צרפת, הולנד ואנגליה	50 שנה
ברית המועצות ומלטה	25 שנה
אלבניה	חיי בן/בת הזוג בצירוף השנים שבהם שבהם גיל כל אחד מילדי המחבר נמוך מ-25.

בעיה חמורה יותר היא הבסיס הפילוסופי של חוק זכויות יוצרים, השונה במדינות רבות באופן מהותי, מהקיים בבריטניה ובארצות הברית. כללית, באירופה נחשבת זכות יוצרים כזכותו של הפרט ובבריטניה היא לא יותר מזכות כלכלית. זכויות הסופרים במדינות האירופאיות (חוץ מבריטניה), המוגנות על פי חוק זכויות יוצרים, מתקיימות מעבר למכירה למוציא לאור. זכויות נוספות אלה מעכבות את השגת האחידות בחוק זכויות יוצרים.

מזה שנים מתנהל ברחבי העולם דיון ממושך בנושא הרפורמה בחוקי הגנת היוצרים, ובכלל זה מאמצים של ארגון הקניין הרוחני, WIPO (World Intellectual Property Organization), שהוקם בג'נבה ב-1978. בקיץ 1983 כינס WIPO נציגי ממשלות וארגונים בינלאומיים לצורך ניסוח טיוטה של אמנה להגנת זכויות יוצרים בתוכנה. למרות שצריכות לעבור חמש שנים בטרם תאושר ותופעל אמנה זו ברחבי העולם, סעיפיה חשובים, כי הם מכסים את התחומים הבאים:

* שימוש לא חוקי בתוכנה.
* העתקת תוכנה.
* פיתוח תוכנה הדומה למוצרים של ארגונים אחרים.

ארגון WIPO המליץ שהחוק יהיה ייחודי לתוכנה, ולא חלק מחוק זכויות יוצרים. הארגון גם המליץ שאכיפת החוק תהיה מאמץ בינלאומי. היה זה ניסיון לשפר את החוק הקיים ולהביא לאחידות בחוקי זכויות יוצרים בכל המדינות. לאחר שבוע של דיונים, הוחלט שטיוטת האמנה אינה מתקבלת ויש להשתמש בחוקי זכויות

יוצרים הקיימים בכל מדינה, לצורך הגנת תוכנה. הקושי בגישה זו הוא שמדינות שונות נמצאות בשלבים שונים של חקיקה להגנת זכויות יוצרים בתוכנה. במערב גרמניה, בארצות הברית ובהונגריה קיימים חוקי זכויות יוצרים ייחודיים לתוכנה ובמדינות אחרות קיימים חוקים בודדים, או שאינם קיימים כלל (מקלנינג, 1983).

למרות שלא הושג סיכום, המשתתפים היו מאוחדים בדעתם בשני נושאים:

(1) יש להגן על תוכנה.
(2) יש להשתמש במודל הדומה לזה של חוק זכויות יוצרים, בידיעה ששאלת הרישום נותרת בלתי פתורה.

עמדה זו נתמכת על ידי ההמלצות ההמתוארות בקווים כלליים בטבלה 10.4. ההמלצות נדונו בשתי קבוצות מומחים במסגרת האגודה הבריטית למחשבים (British Computer Society, גרובר והארט, 1982), בעקבות המסמך הירוק של הממשלה (Cmnd 8302, 1981).

טבלה 10.4 ההמלצות בעקבות דיונים של שתי קבוצות מומחים של האגודה הבריטית למחשבים, באוקטובר 1981

1. דרושה פעולה דחופה להגנת תוכנת מחשב.
2. תוכנה שנכתבה במסוף ונשמרה בשטח אחסון, נחשבת כמשהו חומרי.
3. המרה של עבודה מקורית שנשמרת בהקלטה מגנטית לצורות אחרות של שפת מכונה, היא העתקה של העבודה המקורית.
4. אין להבדיל בין תצוגה על מסך לבין תדפיס (היתה מחלוקת בנושא זה).
5. כל העתקה, גם זמנית, תהיה הפרה של זכויות יוצרים.
6. אפשר לבקש אישור לצורות מפורש לצורות רישום חליפיות של התוכנה המקורית, כדי להחיל גם עליהן זכויות יוצרים.

10.7 הגנה באמצעות עזרים טכניים

יש להשלים את ההגנה המשפטית בעזרת אמצעים טכניים, במצבים הבאים:

(1) הגנה בעזרת תוכניות שירות של היצרן.
(2) חומרה שנבנתה במיוחד לשם כך.
(3) נעילות בתוך התוכנה.
(4) הצפנה.

קיימות דרכים שונות להגנת תוכנה.הגנות מקובלות לדיסקט הן: שינוי כתובות, שינוי סימון המסילות, כיוון של מהירות הסיבוב כדי להשפיע על ספירת הסיביות במסלול, או שילוב של טכניקות אלו (אפל, 1982). ההגנה תהיה מוגבלת כאשר ספק תוכנה משווק תוכניות מקור. לכן, יצרני התוכנה ישתמשו בשיטות אחרות, כמו אספקה של התוכנה בשפת מכונה בלבד.

לעתים מתעורר צורך בהגנה נוספת על תוכנות חשובות באמצעות מנגנוני חומרה מיוחדים. אחד ההתקנים נקרא מחבר ההרשאה ("פלאג"), שמרכיבים אותו באחת הכניסות של מחשב האישי. מחבר ההרשאה מכיל קוד ייחודי שנבדק על ידי התוכנית בכל טעינה שלה לזיכרון. התקן זה מאפשר לעשות עותקי גיבוי מהתוכנית, אך הם לא יפעלו על מחשב שלא מותקן בו מחבר הרשאה. המחבר מגביל את הניידות של התוכנה למחשבים אחרים. התקן חומרה אחר, שמונע העתקה לא חוקית, פותח על ידי עדי שמיר (Adi Shamir). התקן זה גורם לשינוי בדיסקוכתוצאה כל ניסיון להעתקת התוכנה גורם ל"נפילת המערכת.

הגנה על דיסקט באמצעים מיוחדים בפני ההעתקה, אינה מונעת גניבה, אך היא מרתיעה את הגנבים. לדוגמה, הכנסה של גרסה מוצפנת של שם המשתמש בנקודות מסוימות בתוכנה. למשל, תוכנה המופצת על ידי סוכנים תכיל, בצורה מוצפנת, את שם הסוכן ואת שם המשתמש. אם התוכנה תועתק, יופיעו שמות אלה על כל מסך ותדפיס נייר. שיטה אפשרית נוספת היא של נעילות המבוססות על תאריך או מספר הפעלות, אשר גורמות להפסקת הריצה של התוכנית בתאריך מסוים, או לאחר מספר מסוים של הפעלות. המשתמש המורשה יקבל קוד הפעלה חדש והמחזיק בתוכנה שלא ברשות לא יוכל להשתמש בה יותר. שיטה אחרת היא לסמן את תוכנית המקור על ידי הכנסת של קטעים חסרי משמעות, אך ניתנים לזיהוי. בכך יתאפשר זיהוי של תוכנית החשודה כגנובה כאשר משתמשים בה. הקוד יכול לקבל צורה של שגיאה מכוונת, או דרך יוצאת דופן להגיע לתוצאה.

כללית, אמצעי הגנה טכניים אינם מושלמים וגנב מקצועי יוכל

לעקוף, או לנטרל אותם. אפשר לעקוף מחבר הרשאה על ידי מציאה ומחיקה של ההוראות בתוכנית, שבודקות אם הוא מותקן במחשב, או על ידי כתיבת שגרה שתדמה את פעולתו. לכן, במקרים מסוימים, הכרחי להשתמש בהצפנה. אחת השיטות שנמצאות בפיתוח משתמשת במערכת הצפנה המבוססת על המפתח הציבורי (ריווסט ואחרים, 1978). הבעיה היא שלא ניתן להסתיר את מפתח הפענוח על גבי התקליטון, כי מקצוענים יוכלו תמיד לגשת לכל חלקיו. המפתח ישמר באופן בטוח רק בתוך כספת.

אמצעי הגנה טכניים מרתיעים מעתיק חובבן. הפירט המקצועי יעקוף את רוב ההגנות. אם כי, מערכות הצפנה מציעות את ההגנה היעילה ביותר (מהוד ומהוד, 1984).

10.8 מסקנות

מכלול החוקים הקיים - חוקי הפטנטים, חוקי הסודות המסחריים וחוקי הזכויות היוצרים - אינם מספקים הגנה מושלמת לתוכנה. רישום תוכנית כפטנט הוא נושא שנוי במחלוקת. למרות זאת, משפטנים מסכימים על העיקרון שאין לרשום כפטנט תוכנה שאינה חלק ממכונה. חוק הסודות המסחריים מקיף יותר, אך הוא מוגבל לצדדים בהסכם או בחוזה. היתרון העיקרי בזכויות היוצרים הוא בהרתעת משתמשים מלהעתיק תוכנות ללא אבחנה בבעלות. חוק זכויות היוצרים בצורתו הקיימת אינו יעיל, אך רבים סבורים שזכות יוצרים והנגזרות שלה הם המנגנון הטוב ביותר להגנה משפטית.

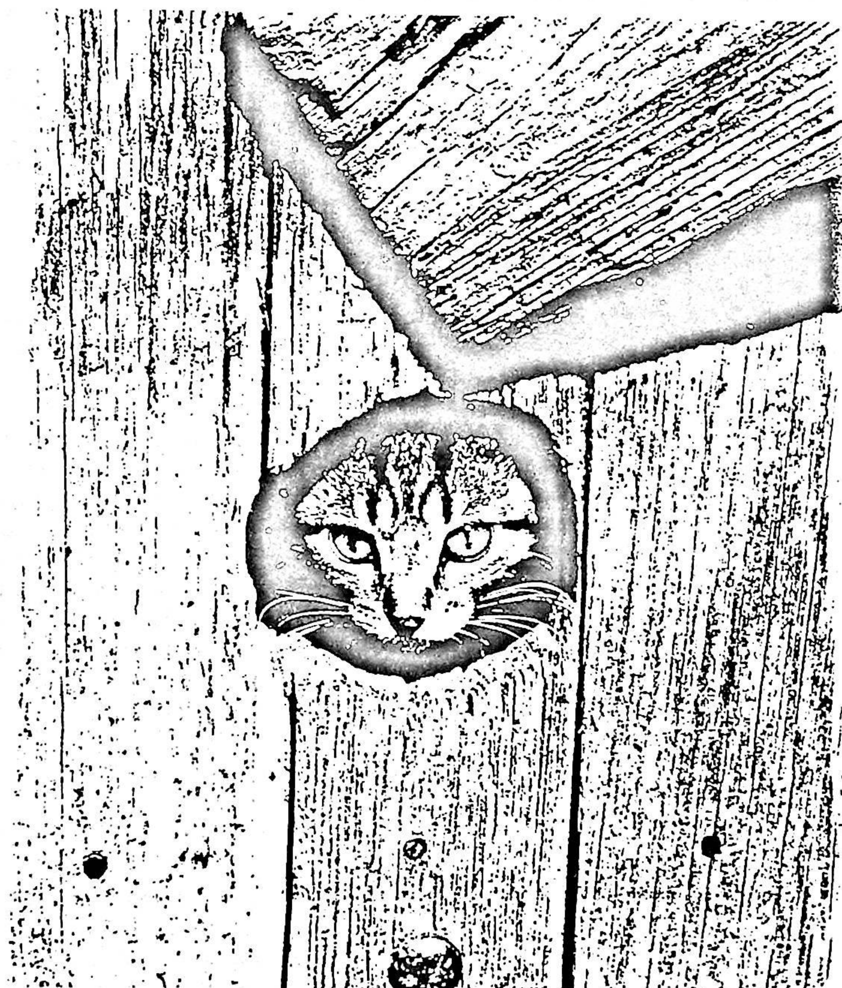
ההתפתחויות הטכנולוגיות יכולות להוביל לתוכנה שתהיה בטוחה לחלוטין בפני העתקות. למרבה הצער, ההתקנים הנוכחיים והחוק הקיים אינם יכולים להבטיח הגנה. לכן, התוכנה הטובה ביותר חייבת להשתמש באמצעי הגנה שמשלבים אמצעי הרתעה רבים, ביחד עם הגנה פיסית. "המסמך הירוק", שפורסם בבריטניה ב-1983, מציין: "אומה כמו בריטניה מסתמכת על העיקרון של קבלת תשלום עבור נכסים רוחניים... יש לנו מסורת של המצאות. היכולת לטעון בעלות על רעיונות היא צעד חיוני בדרך להשגת רווח מהם". תוכנה שווה כסף ולכן, חיוני שאלה המאפשרים הכנסות כספיות מתוכנה יהיו מוגנים מזיוף והעתקות.

שאלות

10.1 מנגנון להגנת תוכנה יכול להיות מבוסס על חוק הפטנטים עם דמי הרשמה נמוכים מאד ועם תקופת הגנה קצרה יותר, באופן יחסי. מהם הקשיים בשיטה זו?

10.2 החוק המוצע ביפן יספק הגנה רק ל-15 שנה ובכך ירתיע עסקים משותפים עם בתי תוכנה מערביים. מהי דעתך?

10.3 ברגע שיפותחו אמצעי הגנה טכניים טובים לתוכנה, לא יהיה צורך בחוקים להגנת תוכנה. מהי דעתך?



פִּרְצה קוראת לגנב

פרק 11

דוגמאות אופייניות לפגיעות באבטחה

בפרק זה יתוארו כמה מקרים אמיתיים. מטרת התיאור איננה לבקר את הארגונים שבהם התרחשו המקרים, אלא לעזור למתכננים של מערכות מידע למנוע כמה מהקשיים שהתעוררו בעבר.

מקרה הקשור לפרטיות יתואר בקווים כלליים, כדי לסייע בהבנת הלחץ שהופעל על הממשלות לחקיקת חוקים להגנת נתונים. מקרה שבו נהרס מחשב של ארגון ידגים את היתרונות שבתכנון לשעת חירום.

ארבעה המקרים הנוספים שיתוארו מדגימים את המקום שתופס המרכיב האנושי במערכת המידע. בכל אחד מהם היתה תקלה, כלומר, מערכת המידע התנהגה בצורה לא מקובלת, שלא נחזתה מראש על ידי מתכנן המערכת. בכל אחד מהמקרים נכשל המרכיב האנושי. באחד מהם המשתמש היה אשם ובאחרים - התנהגו אנשי המקצוע באופן יוצא דופן.

אין בכוונתי לרמוז שקל לזהות אנשים שעומדים להתנהג בצורה יוצאת דופן ולכן, אינם מתאימים לעבוד עם מערכת המידע. הכוונה הפוכה לחלוטין. למעשה, אחד המאפיינים הראוי לציון, של פשעי מחשב הוא מגוון האנשים שמעורבים בתקלה, אשר לרובם אין עבר פלילי. יש לכך השלכות על מנהל כח האדם של הארגון, הנדרש לחוות דעה על מועמדים לעבודה. כל המקרים מדגישים את חשיבות מדיניות הארגון בנושאי מחשוב ובכלל זה: תכנון לשעת חרום, בקרות פנימיות, נוהלי גיוס עובדים ומדיניות השימוש במשאבי המחשב על ידי אנשי עיבוד הנתונים.

11.1 מקרה הקשור לפרטיות

מקרה זה דווח על ידי תוכנית פנורמה ב-BBC. הוא נוגע לבמאית של סרטים תעשייתיים שהפכה למעורבת, שלא באשמתה, בסיוט מהסגנון הקפקאי.

במאית הסרטים הצטרפה לארגון שהתמחה בעשיית סרטים ללקוחות תעשיתיים. זמן קצר לאחר שהתקבלה לעבודה, אמר לה מעבידה

שלקוח, חברת בריטית מובילה בענף הבניה, דיווח שהיא מהווה סיכון בטחוני. חברת הבניה הודיעה שלא תאפשר לה להכנס לשטחה וכמובן שלא תאפשר לה לעבוד עבורה.

במאית הסרטים היתה שבורה לחלוטין. למרות המאמצים שהשקיעה, לא הצליחה לגלות מדוע היא מהווה סיכון בטחוני. היא פחדה שהקריירה שלה עומדת להרס ושהיא לא תוכל לעבוד יותר במקצועה, מכיוון שהמידע שקיבלה עליה חברת הבניה יוכל להגיע גם לחברות אחרות. כתוצאה מכך, חשבו הבמאית ובעלה לעבור לצפון אנגליה ולפתוח מסעדה, או לעסוק בפעילות אחרת, שאינה מחייבת את בדיקת הרקע שלה.

המצב נראה חסר מוצא, אך בניגוד לגורלם של קורבנות אפשריים אחרים, התגייסו לעזרתה שני אנשים בעלי השפעה שהצליחו לפתור את התעלומה. הראשון היה המעביד שלה, שדרן מפורסם ב-BBC לשעבר, שלא היה מוכן לקבל את החלטת הלקוח כפשוטה. הוא רצה לדעת מהו מקור המידע שלפיו העובדת שלו מהווה סיכון בטחוני. הוא יצר קשר עם המחלקה המיוחדת (Special Branch), המורכבת מלמעלה מ-10,000 נושאי משרות בבריטניה. מטה המחלקה המיוחדת בלונדון נמצא במשרדי הסקוטלנד יארד. למחלקה זו משימות רבות, אך הפעילות הרגישה ביותר שלה היא מעקב אחר אנשים החשודים בפעילות נגד בטחון המדינה. המחלקה המיוחדת, בגלל תפקידה, מזכירה במובן מסוים את פעילות ה-CIA בארצות הברית. אין זה מדויק לגמרי, מכיון שאנשי המחלקה המיוחדת הינם חלק מ-CID, האגף לחקירת פשעים וככאלה, הם חלק מהמשטרה. האדם השני שהתגייס לעזרתה הבמאית היה אביה, קצין בכיר בדימוס של הסקוטלנד יארד. חבריו לשעבר במשטרה עזרו לו ליצור קשר עם המחלקה המיוחדת.

תחילת פתרון התעלומת היה בתקרית ירי באמסטרדם, שבה היתה מעורבת כנופיית באדר-מיינהוף ושהציבה את משטרת הולנד בכוננות. באותו זמן בילו הבמאית הסרטים ובעלה חופשה בהולנד. כאשר הגיעו בני הזוג לבית קפה לאכול ארוחת בוקר הם נראו מלוכלכים ועייפים, לאחר שבילו את הלילה על מעבורת מכוניות בדרכם מבריטניה. מלצר חשדן חשב שהבעל דומה לווילי סטולר, טרוריסט מקבוצת באדר-מיינהוף. הוא התקשר למשטרה, מסר להם מידע בנוגע למכונית רנו שבה נסעו שני התיירים ומשטרת הולנד ביקשה את עזרתה של המחלקה המיוחדת בלונדון. המכונית היתה רשומה על שם האשה. המשטרה ביצעה חקירה אודות האשה, אך לא אודות בעלה, בניסיון למצוא קשר לטרוריסטים. החקירות לא נשאו כל פרי. והמחלקה המיוחדת לא המשיכה לחקור בדבר. במאית הסרטים לא נחקרה והמשיכה בחופשתה מבלי שהעלתה על דעתה שהיה נתונה תחת מעקב של המחלקה המיוחדת. למרבה הצער, פרטי החקירה נותרו בתיקי המחלקה המיוחדת.

לאחר שהמקרה הגיע לסיומו הטוב, שאלה במאית הסרטים את קצין המחלקה המיוחדת מה היה קורה לה אילו אביה לא היה מסוגל להשתמש במעמדו כדי ליצור קשר עם המחלקה .והיא היתה נאלצת לשכור את שירותיו של עורך-דין. לדבריה, נענתה שהפרטים לא היו נחשפים, הקריירה שלה היתה נהרסת והיא היתה מבלה את שארית חייה עם תווית של סיכון בטחוני. כל זאת - בגלל טעות.

11.2 עובדים שאינם אנשי מחשב והפגיעות של מערכת המידע

אין צורך בבקיאות במחשבים, כדי להשתמש בהם לביצוע מעשי רמאות. במקרים הבאים, העבריינים היו פקידים מראש הסולם ההירכי שהשתמשו לרעה בשגרת עבודתם במערכות המבוססות על מחשבים. כמו בכל עבירות הצווארון הלבן, גם אלו היו עבירות ראשונות על ידי עובדים שניצלו הזדמנויות שנוצרו על ידי הקורבנות - המעסיקים.. שני מקרים מוכיחים שהטענה שפשעים מבוצעים על ידי קבוצה קטנה של פורעי חוק הניתנים לזיהוי, מוטעית מיסודה.

11.2.1 משתמש מורה למערכת המידע לבצע תשלומים לא חוקיים

מפקח מחלקת תשלומים ברשות מקומית בלונדון גילה שיטה ליצירת מסמכים מזויפים, הכנסתם למחשב והסתרת הפלט. כך שולמו 13,956 ליש"ט בשלושה צ'קים לזכות דיוויד אלן, שם בדוי של בנו של מפקח התשלומים. הבן לקח את הכסף והעביר 2,000 ליש"ט לחשבון של אימו. החשבון היה תחת השם הבדוי ברברה וויט, אך הכתובת היתה כתובתו של המפקח.

כאשר המבקר הפנימי עמד להשלים בדיקה שגרתית של ההוצאות בפועל כנגד התקציב, הוא גילה, לגמרי במקרה, שתי המחאות בלתי מוסברות. כתוצאה מכך נפתחה חקירה. כששמע על מפקח החקירה, ביקש שיתרת חשבונה של "ברברה וויט" תישלח לכתובתה בהמחאה. היא החזירה את המעטפה לבנק מבלי שפתחה אותה ולאחר שרשמה על המעטפה "לא ידועה בכתובת זו". למזלו הרע של העבריין, פעולה זו לא שכנעה את השופט, שדן במקרה זה בשנת 1982. המשפט תואר על ידי העיתונות כמשפט הראשון על עבירה באמצעות מחשב, למרות שכבר בשנות ה-70 התנהלו מספר משפטים דומים.

הבן, שבזבז כמה אלפי ליש"ט בביקורים באוסטרליה וקנדה, הודה באשמה על ביצוע מעשה מרמה, אך האם הכחישה את האשמה. המפקח נמצא אשם ונשלח למאסר של 12 חודשים.

11.2.2 פקידה השתמשה במערכת המשכורות כדי לרמות את רשות הבריאות

המקרה אירע במחלקת תשלומים של רשות הבריאות, המשלמת בסוף כל חודש את הוצאות הרופאים במסגרת משכורתם. אפשרות נוספת לשלם את ההוצאות, דרך מערכת אחרת שלא היתה קשורה למערכת המשכורות המרכזית, נועדה לזרז תשלומים במקרים מיוחדים. אחת מפקידות התשלומים ניצלה מצב זה. הוצאות הרופאים שולמו בדרך כלל באמצעות מערכת המשכורות המרכזית. בכמה מקרים הכניסה הפקידה את ההוצאות דרך המערכת המרכזית וגם במערכת המשנית. כך ביצעה תשלום כפול של אותן הוצאות באמצעות המחאה ידנית, שהגיעה ישירות לשולחנה (ליין ורייט, 1979).

בדצמבר 1977, לאחר שנגנבו כ-13,000 ליש"ט, התגלה מעשה המרמה כאשר הפקידה נעדרה בגלל מחלה. רופא ביקש תשלום של 425 ליש"ט, על פי דרישה שהגיש מוקדם יותר באותו חודש. הוא לא היה מודע לסידור שבו התשלום מתבצע במסגרת המשכורת בסוף החודש. בקשה פשוטה זו חשפה את העובדה שההוצאות שולמו כבר דרך המערכת המשנית בהמחאה ידנית, ולא על שמו של הרופא. מעשי המרמה נמשכו למעלה משנתיים ובמהלכם קודמה הפקידה בזכות מומחיותה, נחישותה ואמינותה. הפקידה הודתה ב-13 מעשי מירמה ונשלחה למאסר של שנה.

11.3 שימוש לרעה במחשב של חברת ביטוח

פרצה באבטחה התרחשה בחברת ביטוח בינלאומית שבסיסה בבריטניה (סמוק, 1982). ב-1981 עברו תשלומי הפרמיות בחברה את מכסת ה-400 מיליון ליש"ט. כדי לנהל את פעילות החברה השתמשו במחשב גדול מסוג IBM/3033, עם מערכת של מסופים מקוונים למשרדי הארגון בדרום-אפריקה, ארצות הברית ובריטניה.

נוהל הכניסה למחשב היה להדליק את המסוף וללחוץ על מקש return. כתגובה, בקשה המערכת מהמשתמש להצביע על היישום, או על שירות אחר שברצונו להפעיל. בשלב הבא הוקש מספר מזהה (sign-on) וסיסמה. המספרים המזהים הוקצו במקום על ידי ההנהלה, אך הסיסמה נבחרה על ידי המשתמש, כדי למנוע שימוש לא חוקי במשאבי המחשב מעבריינים שהשיגו את המספר המזהה. מתכנתים יכלו להכניס, למיין לאחזר ולשמור נתונים, וגם לפקח ולשנות קבצים דרך מערכת חזקה ונפוצה לעבודה מקוונת בשם ROSCOE, המשווקת על ידי Applied Data Research מפרינסטון, ארצות הברית. מחלקת עיבוד הנתונים, שבסיסה היה בערי השדה, היתה אחראית על הפיתוח והתחזוקה של התוכנה ועל אספקת שירותי עיבוד נתונים כלליים.

מנתח מערכות בכיר שעבד בארגון במשך שתים עשרה שנה וראה עצמו כעובד נאמן וחרוץ, היה בחופשה. במהלכה, גילה אחד המתכנתים באקראי רשימה של קבצים ותוכניות בלתי מוכרים בספריית ROSCOE. במהלך החקירה שנפתחה נגד מנתח המערכות, התגלו תוכניות פרטיות לניהול חשבונות ותוכניות למילוי טפסי טוטו, שנעשה בהם שימוש 25 ו-43 פעמים בהתאמה. מנתח המערכות פוטר מעבודתו, אך מאוחר יותר, בדצמבר 1981, פנה בעזרת וועד העובדים לבית הדין לעבודה וטען שלושה דברים:

(א) תוכנית היישום לא שימשה לצרכים עסקיים, כי ניהול החשבונות של העסק של חברתו לחיים, שהתוכנית אמורה היתה לנהל אותם, נעשה באופן ידני, מכיון שמספר הנתונים היה קטן. התוכנה הופעלה לניהול חשבון המשכורת של חברתו המורה בלבד.
(ב) המחשב נוצל לרעה על ידי עובדים רבים.
(ג) לאחר פיטוריו, התגלה עובד אחר שניצל לרעה את משאבי המחשב, אך הוא הושעה מהעבודה למשך שבועיים בלבד.

פיטוריו של מנתח המערכות אושרו בבית הדין לעבודה ולא נקבע לו כל פיצוי.

כתוצאה מהדיונים בבית הדין לעבודה, החליט המגזין Computer Fraud and Security Bulletin לבצע ניתוח מעמיק של האירועים. בסיכום, הוא דיווח על "מצב עניינים חמור הרבה יותר ..." עם "ליקויים חמורים באבטחת המחשב". העובד שהושעה לא הועסק על ידי מחלקת עיבוד הנתונים. הוא היה מנתח מידע בלונדון שעבד במחלקת התכנון והמחקר, שתפקידה לנתח כיוונים עסקיים ולהכין נתונים סטטיסטיים. הוא הועסק בארגון חמש שנים ולפני כן, היה לו ניסיון רב במחשבים, כולל תקופה בה עבד כתוכניתן. הוא הכיר את מערכת ROSCOE ואת האמצעים החזקים והמקיפים שהיא מספקת לניהול שירותי המסופים. אמצעים אלה צריכים לעמוד אך ורק לרשות עובדים מורשים וגם זאת, תחת ביקורת מאוד הדוקה.

לפני הדיון המשפטי, בדקה מחלקת עיבוד הנתונים את רישומי המערכת וגילתה שמשתמש מרוחק נכנס באופן לא חוקי לספריה הפרטית של התוכניתן הראשי. המשתמש זוהה ונמצא שהיתה לו תוכנית שעקפה את אמצעי האבטחה והציגה את תוכנו של כל חלק בספרית הפיתוח. ממצא זה עורר פניקה, מכיון שהתקיימה פריצה למידע רגיש מאוד שהיה אמור להחשף בפני מספר קטן של משתמשים מורשים בלבד.

התוכנית היתה שייכת למנתח המידע שהפיקוח עליו היה בידי עובדים חסרי ידע טכני להשגיח ולמנוע את הפיגוע. הפורץ הזה יכול היה להכנס לתוכנית הערכה, שדירגה את ההנהלה לפי בסיס

של נקודות. אם הנתונים או הקריטריון היו נחשפים, היתה נגרמת מבוכה גדולה במחלקת כוח האדם. הפורץ יכול היה לצבור מידע הנוגע לסוכני ביטוח, לשיטות חישוב של פרמיות ולנתוני שיווק - מידע בעל ערך רב למתחרים. יתר על כן, עם ידע נוסף על תוכנית שירות סטנדרטית של יבמ - SUPERZAP, הוא יכול היה להעלים מקבצי הרישום את הראיות על השימוש במערכת.

החקירה על התנהגות מנתח המערכות התנהלה בגלוי והסתיימה ב"תיק מקיף על פעולותיו הנלוזות", אך החקירה על מנתח המידע התנהלה בסודיות יחסית. מנתח המידע טען שהוא השתמש במומחיות שלו רק כדי לשפר את השירות שקיבלה המחלקה שלו, על ידי שינוי של עדיפות הביצוע בעבודתו. לכן העובד הוזהר ועונשו היה סימלי. המקרה של מנתח המידע, בניגוד למקרה של מנתח המערכות, כמעט ולא קיבל תשומת לב בעיתונות.

11.4 אנשי מחשב גונבים קבצים ודורשים תמורתם כופר

מנהל תפעול ומנתח מערכות עבדו עבור ICI על מערכת יבמ 370/145 ברוזנברג, הולנד. לארגון זה היה אתר חלופי בווינהאבן. מנהל התפעול בדק את נוהלי האבטחה כדי לשפר אותם. להפתעתו, גילה שנקודת התורפה המרכזית של התוכנית היא הוא עצמו, מכיוון שהיתה לו גישה לספריית הנתונים המרכזית ולספריית הגיבוי שהוחזקה באתר החלופי. על מנהל התפעול היה לחתום על טפסים המאפשרים את קבלת הקובץ הראשי ועותק הגיבוי. מנהל התפעול עבד עם שותף שסיפק מומחיות בתוכנה ועזר בזיהוי הקבצים שכדאי לקחת.

שני העבריינים גנבו קבצים ראשיים ועותקי גיבוי שאוחסנו ב-48 אגדי תקליטים ובלמעלה מ-500 סרטים מגנטיים והכילו נתונים חשובים ביותר לארגון (ליין ורייט, 1979). אמצעי האחסון המגנטיים הוסתרו באנטוורפן, בדירה ממוזגת אוויר שנבחרה בזכות התאמתה לאחסון חומר מגנטי. לאחר מכן דרשו השותפים לפשע 275,000 ליש"ט בתמורה להחזרת הקבצים, ואיימו להרוס אותם אם הכופר לא ישולם. הם היו אנשי מחשב מוכשרים, אך התגלו כפושעים שלומיאלים שלא הצליחו להתגבר על מלאכת איסוף דמי הכופר.

השניים טילפנו למנהל בכיר שהיה אחראי על מנהל התפעול, מספר שנים קודם לכן, ודרשו ממנו להשיג את הכסף בשטרות של 5 ו-10 ליש"ט ולשלוח אותו ללונדון. כדי להוכיח את רצינותם, שלחו סרט מגנטי שהמידע שהוא הכיל נמחק באופן חלקי וצרפו קלטת שהכילה הודעה. בהודעה הסבירו מה עשו לסרט ואיימו שכך ייעשה לכל הסרטים, אם לא ימולאו דרישותיהם. הארגון העריך את

הנתונים ב-150,000 ליש"ט וחשש שיידרשו שש שנות אדם כדי לשחזר אותם. העבריינים ניסו לארגן פגישה ברחוב אוקספורד בלונדון, אך היא נכשלה. כשנציג הארגון עמד לעזוב, הגיע הזוג רכוב על גבי קטנוע. הם ניסו לחטוף את התיק שנשא נציג הארגון, כי חשבו שהתיק הכיל את הכסף. הם נאסרו לאחר מרדף שתואר על ידי עיתונות המחשבים כמרדף נוסח "שוטרי קיסטון", מעידן הסרט האילם.

בזמן שמנהל התפעול המתין למשפטו, הוא הצליח להשיג חוזי עבודה בכמה יחידות מחשב. הוא השתמש בשמו האמיתי ופוטר רק לאחר שסיפר למעסיקיו על הקשר לפרשת ICI. מנהל התפעול נדון לשש שנות מאסר ומנתח המערכות - לחמש שנות מאסר, שהופחתו לאחר ערעור לארבע ושלוש שנים, בהתאמה.

11.5 פיצוץ בדוד חימום הורס את חדר המחשב

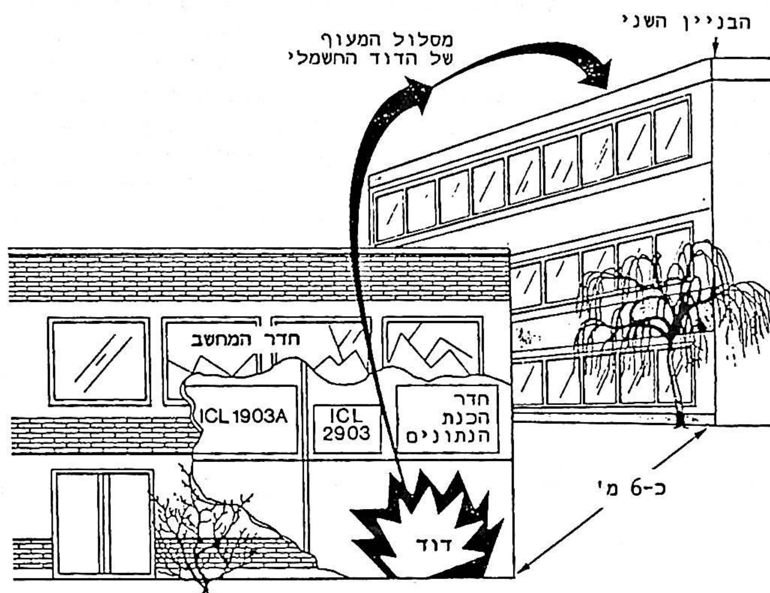
חברה בקנט היתה חסרת מזל. חדר המחשבים שלה נהרס לחלוטין באוגוסט 1977. המקרה מתואר בתרשים 11.1.

בשעות המוקדמות של הבוקר הפסיק לפעול ציוד הבקרה של דוד החימום והצטבר קיטור שגרם לפיצוץ הדוד. דוד החימום, שמוקם מתחת לחדר המחשב, הועף ועבר דרך התקרה שהפרידה בין שתי הקומות. משם המשיך הדוד במעופו ועבר דרך חדר הכנת הנתונים ומשם - מחוץ לבניין, דרך גג הבטון. הדוד סיים את מעופו בגג הקומה השנייה, בבניין שהיה מרוחק כשישה מטרים מהבניין הראשון.

הפיצוץ יצר חור בקוטר של שישה מטרים ברצפה של חדר הכנת הנתונים. שמונה מסופים להכנסה ישירה של נתונים ושמונה מכונות ניקוב נפגעו מהנפילה, או מהפיצוץ. מחשב ה-ICL2903 של החברה נפל לקומה שמתחת ונהרס לחלוטין. בשעות העבודה הרגילות עבדו עשרים איש בשטח שבו נפלה הרצפה, אך למרבה המזל לא נכח שם איש בשעת ההתפוצצות. שני מפעילים של משמרת לילה, שעבדו בסמוך למחשב ICL1903, הצליחו להמלט ללא פגע. מחשב ה-ICL1903 כוסה באבק ובמים ולמרות שלא נהרס, הוא יצא זמנית מכלל פעולה.

סרטים מגנטיים ודיסקים רבים, שהיו קרובים לאיזור שנפגע, נהרסו, אך למרבה המזל היו לארגון קבצי גיבוי שאוחסנו במקום מרוחק מחדר המחשב. כדי לאושש את שירותי עיבוד הנתונים היה צורך למצוא מחשב תחליפי בלבד. יצרן המחשב עזר לארגון למצוא, במרחק 85 קילומטר בערך, משתמש אחר עם מחשב די גדול שיכול היה לקלוט עבודות נוספות. שלושה ימים לאחר ההתפוצצות עברו

שישה מפעילים להתגורר במלון הקרוב למחשב הזמני, כדי לחדש את עיבוד הנתונים. הנתונים הועברו מהארגון למחשב הזמני בעזרת הליקופטר.



תרשים 11.1 התפוצצות שהורסת חדר מחשבים

חדר המחשב הישן לא היה בטוח והיה צורך למצוא אתר חדש. כעבור 15 ימים מיום האירוע, היה חדר המחשב החדש מוכן לשימוש ושירותי המחשוב הוחזרו למצב הנורמלי. המחשב ICL1903 שניזוק תוקן ומערכת ICL1902T החליפה את המחשב שנהרס. קבצי הגיבוי, ביחד עם מימון ומאמץ מועט, הספיקו להחזיר את המצב לקדמותו. למרות חוסר המזל נמנע אסון, כי לארגון היו תוכניות לשעת חירום.

11.6 לקחים מהמקרים

המקרים שתוארו מהווים דוגמאות לבעיות שעלולות להתעורר במערכות מידע המבוססות על מחשב. מטרת הצגת הדוגמאות הללו לא היתה להרגיע ארגונים שיטענו שהם בטוחים יותר. מקרים אלה הובאו כדי שארגונים, מנהלים, משתמשים ומתכננים של מערכות מידע ילמדו מניסיונם של אחרים.

11.6.1 המקרה הקשור לפרטיות

המקרה שקשור לפרטיות משמש אות אזהרה למתכנני מערכות מידע, בהדגישו את העובדה שהמרכיבים האנושיים של המערכות אינם מתנהגים תמיד כמצופה מהם. למרות מסורת המשמעת של המשטרה, ביצע קצין משטרה במקרה המדובר טעות חמורה, שאינה ניתנת להסבר. אפשר לצפות שאנשים הלוקחים חלק בעסקים אזרחיים יתנהגו, לעתים, באופן יוצא דופן ויפגמו בתפעול התקין של המערכת. למרות שהמערכת ששימשה את המשטרה בזמן האירוע המדובר לא היתה ממוחשבת, אפשר להדגים בעזרתו נזקים שעלולים להגרם על ידי הפצת מידע שגוי, ולהדגיש את הצורך בחוקים יעילים להגנת נתונים.

המקרה המדובר גם מחזק את הטענה, כלפי החוק הבריטי במצבו הנוכחי, שאינו מתייחס למערכות ידניות, ושמשום מה המערכות המשטרתיות אינן כפופות לו (גוסטין, 1984). חידה מעניינת, שנותרה בלתי פתורה, היא כיצד הצליחה חברת הבניה להכנס לקבצים של המחלקה המיוחדת, המכילים מידע סודי אישי שגם לנשוא הנתונים אין גישה אליו. יש לקוות שהחוק יפחית מקרים מסוג זה. נושא אחרון ולא פחות חשוב, הם הלקחים שיכולים מתכננים של מערכות מידע ללמוד מהמקרה. עליהם להכיר בפגיעות של אנשים כאשר הם מתכננים מערכות שעומדות בדרישות החוק.

11.6.2 גניבה של מדיה מגנטית

שני אנשי המחשב בני העשרים ושבע, שהועסקו על ידי ICI, הורשעו בגניבת דיסקים וסרטים מגנטיים חיוניים ובדרישת כופר תמורתם. המקרה מאיר את הבעיות שהיו בנוהלי הארגון - בעיות שהיו באחריותו של מנהל התפעול. בזמן הגניבה, מעט מאוד מנהלי יחידות מחשב יכלו לטעון שמקרים כאלה לא יכולים להתרחש ביחידות שלהן. כדי להקטין את הסיכון לפגיעה מסוג זה, מוטל על הארגונים לבצע את הפעולות הבאות:

* להבטיח שהכניסה לקבצים חשובים לא תהיה מרוכזת בידי אדם אחד, גם אם יהיה בכיר, כי אין להניח שעובדים בכירים יתפתו פחות מאחרים לבצע פשע.
* להבטיח, כתנאי מוקדם להוצאת מדיה מגנטית, שיתוף פעולה בין כמה אנשים.
* להחזיק כמה דורות של קבצי נתונים, בדרך כלל - שלושה דורות; להחזיק כל דור במקום אחר, כדי למנוע שאדם אחד יוכל להוציא את שלושתם.
* לדרוש המלצות מכל המועמדים לעבודה ולבצע בדיקות רקע היכן שנדרש.

11.6.3 מקרים שמעורבים בהם אנשי מחשב לא מקצועיים

במקרים רבים תלויה האבטחה ברצונם הטוב של האנשים, יותר מאשר ביעילות אמצעי ההגנה. למרות זאת, אין להתעלם מעקרונות שנקבעו על פי ניסיונם של רואי חשבון מקצועיים במאה השנים האחרונות. היתה זו הטעות העיקרית בשני מקרים שמעורבים בהם אנשי מחשב לא מקצועיים. הפיתויים שעמדו בפני שני העובדים היו קטנים מאוד וסביר להניח שהפשעים היו נמנעים, לו נקטו הארגונים באמצעי הזהירות הבאים:

* הגדרה ברורה של אחריות העובדים והפרדת תפקידים מתאימה.
* עובדים בפונקציות שונות ישתמשו במשרדים נפרדים, או בחלקים שונים של אותו משרד, כדי למנוע שיתוף פעולה בין אנשים בפונקציות שונות.
* הערכת הסכנה הקיימת במערכת תשלומים כפולה.
* ביצוע נכון של בדיקה ובקרה של הכנת חשבונות ותשלומים.

11.6.4 שימוש לרעה במשאבי מחשב

קשה להעריך במדויק את ההיקף והתדירות של השימוש לרעה במשאבי מחשב. התמונה שצוירה לגבי שנות ה-70 על פי נתונים סטטיסטיים שנאספו על ידי מרכז המחשבים הלאומי בבריטניה תואמת את הנתונים שנאספו במשך השנים 1981-1976 על ידי יחידת הפיקוח הממשלתית. המחקר של מרכז המחשבים הלאומי מדווח רק על שני מקרים של שימוש ללא הרשאה, מתוך 142 משיבים. המחקר של יחידת הפיקוח הממשלתית, המבוסס על 319 משיבים (ראה גם טבלה 11.1), מדווח על שנים עשר מקרים של עבודה פרטית, המייצגים אובדן של כ-16,000 ליש"ט, ושני מקרים של גניבת זמן מחשב המוערכים ב-500 ליש"ט.

שני המחקרים מצביעים על רמה נמוכה יחסית של שימוש לרעה במשאבי מחשב, אך הרמה בפועל ודאי גבוהה יותר. כמו במקרה של חברת הביטוח המתואר בסעיף 11.3. מסתבר שחברות, במיוחד בסקטור הפיננסי, אינן נוטות לדווח על פגיעות באבטחה, כי בעלי המניות עלולים לדאוג להשקעתם ולגרום לעריפת ראשים, ולאו דווקא של מבצעי הפשע. במקרה של חברת הביטוח, הפעולות הבאות עשויות להקטין את הסיכונים (שמוסיק, 1982):

(1) קביעת מדיניות החברה לשימוש פרטי במשאבי המחשב.
(2) להבטיח שהעובדים יהיו מודעים למדיניות זו ושיינקטו צעדים משמעתיים כנגד המפירים.
(3) להגביל את הגישה לתוכנות ואת השימוש בתוכניות שירות, כמו SUPERZAP.

(4) ביצוע רישום כרונולוגי של הפעולות (log) וגם בדיקה שגרתית ותדירה של הרישומים האלה.

טבלה 11.1 מקרי גניבה ושימוש לרעה במשאבי מחשב, לפי מחקרי יחידת הפיקוח ו-וועדת הביקורת.

	המחקר של 1981, שמקיף חמש שנים ו-319 משיבים		המחקר של 1984, שמקיף חמש שנים ו-943 משיבים	
סוג הפעילות	מספר המקרים	אובדן כולל (ליש"ט)	מספר המקרים	אובדן כולל (ליש"ט)
עבודה פרטית	12	16,339	11	2,220
גניבת זמן מחשב	2	500	1	71
גניבת תוכנה	2	500	-	-
גניבת פלט	2	40	2	-
חבלה	3	-	-	-
פגיעה בפרטיות	1	-	-	-
סה"כ	22	17,379	17	2,291

הנושא האחרון הוא אולי החשוב ביותר. המקרה של חברת הביטוח מהווה דוגמה מושלמת להסתמכות על בקרות טכניות בלבד - סיסמאות והצפנה - והתעלמות מוחלטת מהצורך בפיקוח. מצב זה נפוץ אצל טכנוקרטים בענף המחשבים, שמתעלמים מאמצעי הגנה חזקים ופשוטים, המבוססים על מערכות ידניות, לטובת מנגנונים מתוחכמים מבחינה טכנית. המקרה שבו נהרס מחשב של ארגון בהתפוצצות מדגים את היתרונות שבמדיניות פשוטה, אך יעילה.

11.6.5 מחקרים על פשעי מחשב

קשה להשיג מידע על ההיקף האמיתי של השימוש לרעה במחשב, בגלל חוסר הרצון הטבעי של ארגונים לספק מידע שעלול להרשיע את ההנהלה באי הפעלה של בקרה מתאימה. כדי להעריך את הסיכון שבשימוש לרעה במחשב, השלימה יחידת הפיקוח הממשלתית בשנת 1981 את מחקרה הראשון בנושא פשעי מחשב בבריטניה (קימנס, 1981). בשנת 1984 השלימה וועדת הביקורת, הגוף שבא במקום יחידת הפיקוח, מחקר שני (וועדת הביקורת 1985). נתונים משני

המחקרים, המבוססים על תשובות של משתמשים מהסקטור הפרטי והציבורי, מוצגים בטבלאות 11.1, 11.2 ו-11.3. מסקנה אחת שעלתה מהמחקרים היא, שבאף אחד מהמקרים לא נעשה שימוש בכישורים טכניים יוצאי דופן וברובם נוצלו נקודות התורפה של הנוהלים הקיימים.

מסקנה שניה (ראה טבלה 11.3) היא שיותר משליש מהמקרים לא התגלו על ידי נוהלי בקרה שגרתיים. למרות שארגונים נעשים מודעים יותר לאבטחה, על אנשי מחשב לקחת בחשבון שפגיעות רבות באבטחת המחשבים מתגלות במקרה, והאבטחה תלויה במידה רבה ביושרם ובאמינותם של העובדים. לכן, על הארגונים לפתח מדיניות מקיפה ומפורטת לאבטחה של מערכות המידע. המחשב והמידע הנמצא בו הם נכסים בעלי ערך לארגון ויש להגן עליהם באותה מידה של תשומת לב הננקטת לגבי כספת בבנק, אם כי אין זו משימה קלה. ניסיון העבר הוכיח את החשיבות והתמורה של מערכות מידע המבוססות על מחשב, את הכוח שהן מעניקות לאנשים שמכירים את פעילותן של המערכות ואת האחריות הכבדה המוטלת על כתפי אנשי המחשבים המתכננים מערכות מידע.

טבלה 11.2 סוגים כלליים של פשעי מחשב

	המחקר של 1981		המחקר של 1984	
סוג הפעילות	מספר המקרים	אובדן כולל (ליש"ט)	מספר המקרים	אובדן כולל (ליש"ט)
שינוי לא חוקי בקלט	42	858,170	58	901,001
הרס, גניבה, או שימוש שגוי בפלט	2	3,600	2	230,185
גניבה, שינוי בקובץ ראשי	1	26,000	-	-
גניבה, או שימוש לרעה במשאבי מחשב	22	17,370	17	2,301
סה"כ	67	905,149	77	1,133,487

טבלה 11.3 שיטת הגילוי של פשעי מחשב

	המחקר של 1981		המחקר של 1984	
התגלה באמצעות	מספר המקרים	יחס %	מספר המקרים	יחס %
- בקרה פנימית	28	42	40	52
- ביקורת פנימית	4	6	9	12
- ביקורת חיצונית	1	1	-	-
- אמצעים אחרים	34	51	23	30
- לא דווח	-	-	5	6
סה"כ	67	100	77	100

שאלות

11.1 "איך ניתן להניע טכנוקרטים עצמאיים ויצירתיים שאינם יודעים לעתים קרובות לקבל מרות, למלא אחר נוהלי האבטחה והבקרה?" (Computer Fraud and Security Bulletin). מהי דעתך?

11.2 מנתח המידע, במקרה של חברת הביטוח, אמר שפיצח את מערכת ההגנה כתרגיל אינטלקטואלי בלבד. "ניתן להשוות זאת לאדם המתגלה ביום ראשון בבוקר בכספת הבנק עם מפתח תואם, וטוען שכל העניין הוא אתגר אינטלקטואלי." (Computer Fraud and Security Bulletin). מה דעתך?

11.3 ההנהלה צריכה לדאוג מכך שמספר גדול של פגיעות באבטחה מתגלה במקרה. מהי דעתך?

11.4 לאחר שקרא את המקרה של חברת הביטוח, טען סטודנט אחד שפיטוריו של מנתח המערכות לא היו מוצדקים. לפי דעתו הוא השתמש במחשב שלא היה פעיל - או בקיבולת העודפת שלו שלא היתה מנוצלת - לכן לא נגרמה למעסיק כל הוצאה נוספת. מהי דעתך?

11.5 יצרן מחשבים אומר: "איננו מוכנים לפתח אמצעי אבטחה נוספים, עד שהמשתמשים ידרשו זאת מאתנו". (Computer Fraud and Security Bulletin). מהי דעתך?

פרק 12

נושאים נוספים לדיון

במהלך שני העשורים האחרונים השתנתה זירת המחשבים בהתמדה. שינויים תכופים והתפתחויות בטכנולוגיית המידע יגרמו לארגונים, קטנים כגדולים, למחשב פונקציות שבוצעו עד כה באופן ידני. כך יתוספו לארגון נכסים בעלי ערך, שכמה מהם, שאינם ניתנים להחלפה, מיוצגים באופן אלקטרוני. מבחינת האבטחה, המשמעות של הרחבת השימוש בטכנולוגיית המידע בעסקים, היא התגברות החשיפה לאיומים. האיומים שצפויים מעברייני הצווארון הלבן עלולים לגרום אובדן באמצעות גניבה, מעילה, מעשה מרמה וחבלה. הסכנות הגוברות, בשילוב עם הרחבת השימוש בטכנולוגיית המידע יוצרים סביבה אשר בה:

* גדל הצורך בעובדים אמינים, בעלי מודעות לאבטחה.
* מתפתחים סוגים חדשים של נכסים שייחשפו לאיומים, של עבריינים שעלולים להשתמש בשיטות תקיפה חדשות.
* משך הזמן הנדרש לגילוי ולניצול פרצות באבטחה משתנה משבועות וימים לשניות וחלקי שניות.
* הפגיעה באבטחה אינה מוגבלת לאיזור גיאוגרפי אחד. היא יכולה להתבצע דרך רשת התקשורת מאתר המרוחק קילומטרים רבים ממקום האירוע.

אם התרחיש שתואר יחליף את המצב העסקי הקיים, שבו אחוז גבוה של האובדנים נגרם מאירועים בשוגג, סביר להניח שבעתיד נראה מצב שונה:

* יתרבו הפגיעות באבטחה, כתוצאה מהגידול בכמות המחשבים ומהרחבת השימוש בטכנולוגיית המידע בפעילות העסקית.
* יישומים חדשים של טכנולוגיית המידע ייצרו פגיעויות חדשות ויספקו מנגנונים חדשים לביצוע פשעי מחשב. לדוגמה, מערכות אלקטרוניות להעברת כספים (EFT) מעבירות מיליוני ליש"ט מדי יום בבריטניה ומחוצה לה. פרצה במערכת מסוג זה עלולה לאפשר הלבנת כספים זריזה ומעשי מרמה אחרים.
* הגדלה משמעותית של האובדן, בגלל פגיעות חמורות באבטחה (פרקר ואחרים, 1984).

כדי להתגבר או לנטרל בעיות אלו, על הארגון לקיים תוכנית אבטחה שתכיר בחשיבות של היערכות איכותיות ובגישה מערכתית

12.1 תוכנית אבטחה בארגון

המחשוב הוערך בעבר, ללא הצדקה, כבלתי מזיק וללא כוונות זדון. היום מכירים בפוטנציאל הקיים בו למעשים פליליים ותקלות בשגגה. הובן הצורך באבטחה, במיוחד כאשר המידע רגיש ובעל ערך, כמו נתונים אישיים ונתונים המייצגים סכומי כסף גדולים, או סודות מסחריים, שמועברים בצורה אלקטרונית. במערכות צבאיות גורמי איומים אפשריים הם התקפות טכניות מתוחכמות ואנשים. יש להקצות משאבים כספיים ואנושיים רבים להגנה על המידע. כללית, המצב בעולם העסקים הפוך למצב הצבאי. המאמץ הטכני לפרצה קטן ולא משמעותי והאיום העיקרי למערכות מידע ממוחשבות הוא האנשים המורשים להשתמש במערכת ויודעים כיצד לנצל אותה.

מצב זה עשוי להשתנות בעתיד, אך בינתיים קיים מגוון של מנגנונים טכניים ובקרות מנהליות ונוהליות שיכול להרתיע עבריינים פוטנציאליים. הסכנות האמיתיות למערכות עסקיות אינן נובעות מהפגיעויות של מנגנוני ההגנה. מקורן בחוסר מחויבותו של הארגון לייחס לאבטחת המידע את החשיבות שניתנת להגנה על נכסים אחרים שבבעלותו. תופעה זו מודגמת בסקר שערך Datapro (1985) בלמעלה מאלף יחידות מחשב. במהלך הסקר התברר שליותר ממחצית יחידות המחשב אין תוכנית לשעת חירום, וכמעט רבע מהן אינן מתכוונות לפתח תוכנית כזו.

12.2 הערכות איכותיות וגישת המערכות

אמצעי ההגנה הדרושים להגנה על מערכת המידע בפני עבריין, שעלול לנצל אותה לרעה, צריכים להיות מגוונים ומקיפים בהתאם להתקפות האפשריות (אשבי, 1976). למרות הקושי הטמון באתגר זה, ארגון שמתכוון להגן על מערכת המידע שלו, יוכל לגבש ולהפעיל תוכנית הגנה מתאימה, מורכבת ומשולבת שתכיל אמצעי הגנה טכניים, מנהליים וארגוניים. בתהליך הפיתוח של אמצעי האבטחה תיתכן חשיבות לניתוח איכותי, אך בהיבטים רבים של האבטחה יש צורך באיזון מורכב של הערכות, הכולל:

* הערכת האיומים, אם הם מכוונים ובין אם בשוגג ובכללם המניעים והיכולת של התוקפים.
* אומדן של ערך האובייקטים המוגנים.
* הערכה של יעילות אמצעי ההגנה.

האבטחה דומה באופיה להחלטות עסקיות רבות אחרות, בסיכון שיש לקחת על סמך הערכות איכותיות. יש לשתף אנשים רבים בפתרון בעיות מסוג זה, כמתואר בפרק 8. בין השיטות התומכות בכך: בדיקה של בעלי מקצוע, ניתוח תרחישים, תכנון משותף ומתודולוגיית צ'קלנד. באבטחה נדרשת גישה כוללת. בתחום המחשוב, אין נושא המתאים יותר להכרת הארגון מאשר הגישה המערכתית לאבטחה, אשר מתבטאת למשל במתודולוגיית צ'קלנד.

12.3 מחשבים אישיים

בשנים האחרונות קיימת עלייה נמשכת במספר המחשבים האישיים בארגונים, שבמקרים רבים זו פגישתם הראשונה עם עולם המחשוב. לגידול במספר המחשבים האישיים כמה יתרונות והחשוב שבהם - ענף המחשוב הופך לתחום עממי, שבו אנשים שלא היה להם קשר למחשבים הופכים למשתמשים.

ניידות המחשבים האישיים, באמצעות רשתות מקומיות וחיצוניות במערכות של שיתוף זמן, גרמה לכך שהמחשב נכנס לכל משרד בעולם העסקים והמסחר. בנוסף, הניידות מאפשרת להוציא את המחשב מן המשרד ולהמשיך את העבודה בבית. שיתוף הזמן במערכת כזו שונה מזה של המחשבים הגדולים, מכיון שלכל משתמש יש מעבד משלו. למרבה הצער, למחשב האישי חסרונות מבחינת האבטחה, אשר עלולים לגבות מחיר כבד. אחד החסרונות הוא ההתעלמות מנוהלי האבטחה ומכללי ניהול יעילים, שהתפתחו במשך העשור האחרון במחשבים גדולים. משתמשים במחשבים אישיים אינם ערים, בדרך כלל, לסכנות הקיימות במחשוב. הם סבורים שהסכנות היחידות הן מגניבה של חומרה ו/או תוכנה ונוטים להתעלם מהעובדות הבאות:

(1) ערכו של המידע המאוחסן על תקליטון יכול להיות גבוה בהרבה מערך המחשב עצמו.
(2) רוב בעיות האבטחה שנידונו בספר זה קיימות לא רק במחשבים גדולים, אלא גם במחשבים אישיים.

יש הטוענים שהמחשבים האישיים החזירו את מצב המחשוב לשנות ה-60, בכל הנוגע לאמצעי אבטחה (היילנד, 1983). הבעיות של המחשבים האישיים הן בעיות עם אנשים ובעיות טכניות.

אחת התוצאות של השימוש במחשבים אישיים היא שפחות אנשים משתמשים בכל מחשב. עובדה זו מבטלת כמעט לחלוטין את האפשרות להפרדת תפקידים. משתמש אחד יכול להכניס נתונים, לתכנת ולהפעיל את המחשב והסכנה בכך ברורה. בנוסף, אמצעי הרתעה אחרים, כמו ביקורת אינם בנמצא, כי מחיר הביקורת גבוה ביחס למחיר הציוד.

נקודות תורפה טכניות גורמות, כמודגם בטבלה 12.1, לכמה מבעיות האבטחה. לדוגמה, תוכנות המערכת פשוטות באופן יחסי, ולכן הן פגיעות יותר מהחומרה. מערכת ההפעלה אינה מספקת עבודות, אבטחת קבצים וספריות, או בקרת מסוף - וזה, הדעות, בסיס רעוע למערכות מידע המבוססות על מחשב. מו אישיים רבים מציעים הגנה באמצעות מערכת סיסמאות פ באופן טבעי, מנגנוני הסיסמאות הללו אינם מתוחכמים כמו שנמצאים במחשבים הגדולים. מכיון שהמערכת אינה רושמת את השימוש, קשה לאתר ניסיונות חוזרים ונשנים להכנס אליו עלולים להצביע על ניסיונות חדירה לא חוקיים. כדי לספק יציבה ובטוחה, הצוות המקומי צריך להשגיח על המקום שבו נמצא הציוד, כדי לגלות איומים ולהרתיע עבריינים פוטנציאליים.

טבלה 12.1 פגיעויות ובקרות

הפגיעויות	הבקרות
שיטות הגנה בעזרת סיסמאות	להשגיח וכך אפשר יהיה לגלות ולהרתיע.
מחיקת קבצים מתים	להשתמש בתוכנית שמבצעת מחיקה פיסית של כל הרשומות שיצאו מכלל שימוש.
תוכניות שירות חזקות	להגביל את השימוש החופשי בתוכניות שירות אלו.
אין מבצעים גיבוי קבצים	לשפר את ההדרכה והנוהלים.

פקודות מחיקה ותוכניות שירות הן בעיות נוספות במחשבים האישיים. ברוב מערכות ההפעלה של המחשבים האישיים המחיקה אינה פיסית, היא מתבצעת על ידי הצבת סימן במדריך של התקליט. משתמשים חייבים להיות מודעים לכך ולהשתמש באמצעי הגנה אחרים, או בתוכניות שמבצעות מחיקה פיסית, או כותבות נתונים חסרי משמעות כחלק מפקודת המחיקה.

תוכניות השירות החיצוניות ואלו שמהוות חלק ממערכת ההפעלה מעניקות כוח רב למשתמש במחשב. בעזרתן, אפשר לארגן מחדש את התקליט, לשנות את שם הקובץ, למחוק את הקובץ, להעתיקו ועוד. תוכניות השירות מאפשרות גם לבטל את מחיקת הקובץ (אם לא בוצעה מחיקה פיסית); לגשת לכל סיבית בתקליט ולשנות אותה; לטפל בנתוני הניהול של התקליט, כמו אלה שנמצאים בטבלת

הקצאות הקבצים, במדריך ובטבלת נתוני מחיצה. יש, כמובן, גם גישה ישירה לקבצי תוכניות ולנתונים. בנוסף, אי אפשר למנוע מתוכניות של משתמש לשנות חלקים ממערכת ההפעלה ולעקוף את אמצעי הגנה של המערכת. לכן, יש למסור עותקים של תוכנות מסוג זה לעובדים מורשים בלבד.

אם קיימת מחויבות ארגונית ורמה סבירה של מומחיות, אפשר להתגבר על הקשיים שתוארו לעיל. התוצאה תהיה סביבת מחשב אישי בטוחה יחסית עם חריג אחד - אין הפרדת תפקידים. וועדת הפיקוח הממשלתית הכירה בכך ואמרה שהאטרקטיביות של המחשב האישי תוביל באופן הדרגתי להפסקת השימוש באמצעי בקרה בסיסי, בהפרדת תפקידים (קימנס, 1981).

12.4 תכנון טוב - ערובה למערכת בטוחה

לאחר התקופה שבה נחשבה האבטחה לעניין שולי וכ.. חשוב בפיתוח מערכות מידע המבוססות על מחשב, הגיעו מתכננים וארגונים רבים להכרה שמערכת מידע מתוכננת היטב צריכה לשלב מרכיבי אבטחה וליצור סביבה בטוחה. אין להתעלם מהעובדה שארגונים רבים אינם מקצים משאבים מספיקים להגנה על מערכות המידע שלהם, ואינם ערים לסיכונים הפוטנציאליים שבמחשוב.

יקר מאוד, אך אפשרי, ליצור מערכת מוגנת לחלוטין. ברוב המקרים שבתחום העסקי אפשר להגיע לרמות גבוהות של אבטחה בהשקעה קטנה ולא משמעותית, ביחס לאובדנים הצפויים מהיעדר באמצעי אבטחה. אבטחה היא מרכיב בסיסי בתכנון של מערכות מידע המבוססות על מחשב, אך לא נמצא מתכון אחיד ומוסכם לבצע אותה. כפי שאמר דון פרקר, "השיטה היעילה ביותר צריכה להתייחס לאבטחה כאל משחק שכלליו נקבעים על ידי האויב, ולא על ידי המומחה לאבטחה" ולכן, מתכנן המערכות חייב להיות יצירתי לפחות כמו העבריין הפוטנציאלי.

ספר זה ניסה להציג את המורכבות ואת ההיקף של האבטחה במטרה לספק למתכנן הבנה מלאה בבעיות בסוגיות ובנושאים אלו. כל נסיון לבודד חלקים מן המערכת ולהגן עליהם מבלי לראות את התמונה הכוללת, יגרום לתוכנית אבטחה לקויה ובלתי מתאימה. תוכנית אבטחה יעילה חייבת לשלב שיטות וטכניקות שונות המייצגות את האיזון שבין אבטחה מושלמת לבין התועלת למשתמש.

שאלות

12.1 "אין תשובה אחרת לפשעי מחשב מלבד גיוס אנשים ישרים, אמינים ואחראיים, כדי שכמות האנשים שיפנו לפשע בתחום זה תקטן ככל האפשר." (ג'. האמינג, במכתב לגארדיין, 1983). מהי דעתך?

12.2 קיימות היום גישות וטכניקות מצוינות לאבטחה, כמו מטפי גז הלון והצפנה, ונראה שהאבטחה נמצאת בהישג יד. מהי דעתך?

12.3 בחר שלושה מחשבים אישיים שיש לך גישה אליהם והשלם מחקר התואם לסעיפים המופיעים בשאלה 3.15 (עבודה קבוצתית).

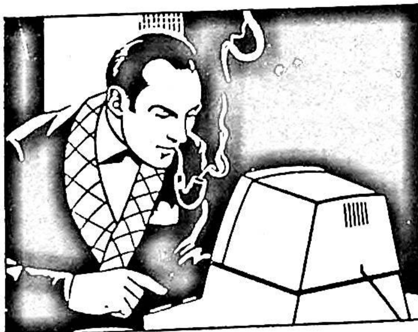
12.4 ההנהלה הבכירה בארגון מסוים תומכת בתוכנית לשעת חירום. מתרחש אסון וההנהלה נחלה אכזבה, כשגילתה שהארגון לא היה ערוך לו, למרות שהיא האמינה שהוכנה תוכנית הולמת לשעת חירום. במה, לדעתך, שגה הארגון?

12.5 התבקשת להעיר על ההצעה הבאה, הנוגעת לאבטחה במחשבים.
ההצעה: להתקין מחשבים אישיים במשרדים של עובדים סוציאלים, כדי לאחסן פרטים על אנשים שהם מטפלים בהם, או שטיפלו בהם בעבר. מדובר במשרדים של רשות ציבורית, שבה והעובדים מחליפים עבודה ו/או מטופלים. כדי שהעובד ימשיך בטיפול, עליו לשלוף את כל המידע שנאסף על ידי קודמיו. כדי שדרישה זו תוכל להתממש, הוצעה מערכת המתבססת על מחשבים אישיים.

העובדים הסוציאליים אחראים על איזור גיאוגרפי קטן יחסית, שבתוכו יכול עובד סוציאלי יחיד להכיר את האנשים שמטופלים על ידי עובד סוציאלי אחר, אך הפרטים המיוחדים לכל מטופל חסויים בפני שאר העובדים ואפילו בפני המנהלים. מידע על מטופל מסוים ישוחרר בשעת הצורך בלבד.

נתוני המטופלים שעומדים להיות מאוחסנים במחשב נוגעים לפגיעות מכוונות בילדים ותינוקות.

מהן לדעתך ההשלכות של פתרון המבוסס על מחשבים אישיים?



נספח א

מערכות מידע ממוחשבות והמשפט בישראל

1. **מערכות מידע והמשפט הישראלי**, עו"ד גדי אופנהיימר.
2. **חוק אבטחת הפרטיות ודרכי יישומו**, הבהרות איל"א, 1987. (*)
3. **כללים לאבטחת מידע**, על פי המלצות המועצה המייעצת לענין הגנת הפרטיות, 1987.
4. **חוק הגנת הפרטיות**, התשמ"א - 1981. (*)
5. **תקנות הגנת הפרטיות** (תנאים לעיון במידע וסדרי הדיון בערעור על סירוב לבקשת עיון), התשמ"א - 1986.
6. **תקנות הגנת הפרטיות** (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו - 1986. (*)
7. **תזכיר חוק המחשבים** (עבירות, הגנת תוכנה וראיות), התשמ"ז - 1987.

(*) הערות:

נספח 2 הוכן על פי המסמך המקורי של איל"א.
נספחים 4 ו-6 כוללים רק את פרקי המבוא (הגדרות) של החוק והתקנות.
נספח 5 הוצג כאן לשם השלימות בלבד, ולא הובא בגוף הספר.

המעוניין במסמכים אלה בשלימותם, יפנה להוצאה.

מערכות מידע והמשפט הישראלי

עו"ד גדי אופנהיימר

מבוא

התפתחות המחשבים בשלושים השנים האחרונות נתפסת בעיני רבים כתופעה המקבילה בחשיבותה למהפכה התעשייתית. אפשר לכנות את החדירה המסיבית של המחשוב לכל תחומי החיים כמהפכת המידע. מהפכה זו, בנוסף להשפעתה על רמת החיים, מביאה איתה גם מושגים ותופעות חדשות שאיתן צריכה החברה להתמודד. להלן, כמה דוגמאות:

(1) אם עד כה מושג הבעלות התייחס בעיקר לשני סוגי דברים, מקרקעין ומטלטלין, הרי שבעידן המחשב נוצר המושג של בעלות בתוכנה, מידע וקבצים, כאשר אלה אינם מקרקעין ואינם מטלטלין, אלא אותות אלקטרוניים בלתי מוחשיים.

(2) המחשוב הביא עמו סוגי התנהגות חדשים. נוצרו אפשרויות פשיעה שלא היו קיימות קודם לכן, כגון השגת כספים, או טובות הנאה אחרות, באמצעות תוכנות וחדירות לא מורשות למאגרי מידע. החלה גם תופעה של שיבוש נתונים. למשל, שיבוש תוכן נאום שהוכן על גבי מחשב עבור אישיות פוליטית בכירה, החדרת מאמר מפוברק למחשב במערכת עיתון ועוד. נוצרו גם הוירוסים שפוגעים בקבצים ובתוכנות.

(3) המחשב הוסיף מימד חדש בתחום הסכנות לחופש הפרטיות. כמות הנתונים האדירה שנצברת אצל גופים שונים, מהירות העיבוד של הנתונים ואפשרויות המיון והשליפה יוצרות איום על הפרט בהיקף ובעוצמה שכמותן לא ידעה האנושות קודם לכן.

(4) נוצרו סוגי עסקים חדשים, כמו למשל, לשכות שירות, החכרת מחשבים ותוכנה, בתי תוכנה שמוכרים פתרונות מדף או תופרים פתרונות לפי מידה, רשתות תקשורת ציבוריות ופרטיות להעברת נתונים, כמו ישראנט וסיפרנט. לעסקים אלה דרושים גם חוזים מיוחדים שמתייחסים ליחסים שבין המתקשרים.

(5) התפתחו מקצועות חדשים בתחום התכנות, ניתוח מערכות, ארגון ושיטות, אבטחת מידע, ביקורת ובקרה, ניהול, הנדסה, תקשורת ועוד.

(6) עד היום הכרנו בעיקר שני סוגים של אמצעי הוכחה בבתי המשפט: העד האנושי והמסמך שכתוב בידי אדם. בתקופת המחשוב נראה יותר משפטים שבהם יהיה צורך להתייחס לפלט מחשב ומדיה מגנטית שמכילה נתונים המשמשים חלק ניכר מהראיות.

דוגמאות ספורות אלו ורבות אחרות מחייבות הסתגלות והתאמה של המערכת

המשפטית. מטבע הדברים, מפגר עולם המשפט אחר ההתפתחויות הטכנולוגיות והמדעיות שכן לא ניתן, ולא כדאי, לחוקק בפזיזות חוקים חדשים בעקבות כל שינוי טכנולוגי ומדעי. עובדה זו נכונה בכל תחום, ולא רק בתחום המחשוב. כך למשל, נוצר פיגור גם בתחום הגנטיקה והפריון. ההתפתחות המדהימה בנושאים אלה, כמו למשל, הפריות מבחנה, הקפאת זרע, "רחם להשכיר" וכיו"ב, יוצרים מצבים שאין להם תשובות ברורות בחוק ובבתי המשפט, ותעבור תקופה לא קצרה עד שהדברים יוסדרו.

התאמת המערכת המשפטית לחידושי מדע וטכנולוגיה בכלל ולנושא המחשוב בפרט, נעשית בשני שלבים. בשלב הראשון אין עדיין חקיקה מיוחדת שמסדירה נושא מסוים ועל מנת שלא לעצור את הקידמה, מבצעים השופטים תרגילי לשון ופרשנות, שבאמצעותם הם מכניסים נושאים חדשים לחוקים קיימים. במלים אחרות, הם מרחיבים את היקף החוק הישן ומכניסים תחת כנפיו את המושגים החדשים שיצרה התקופה. השלב השני והמתקדם יותר הוא שלב הדרגתי של חקיקה מיוחדת שבה יוצרים חוקים ותקנות המתייחסים באופן ישיר למחשב, לתוכנה ולמשתמש מהם.

הסנונית הראשונה של חקיקה ישראלית מיוחדת בנושא המחשוב היא חוק הגנת הפרטיות, משנת 1981 והתקנות שהותקנו על פיו ב-1981 וב-1986. בשנת 1987 הוכן במשרד המשפטים תזכיר חוק המחשבים. התזכיר מטפל באופן מקיף ומפורט בנושאים של עבירות מחשב, הגנת תוכנה והקבילות המשפטית של פלט המחשב. התזכיר הופץ לעיון ולהערות של גופים שונים, אולם עד היום הוא לא הגיע לשלב חקיקה בכנסת. ב-1988 נעשה תיקון לחוק זכויות יוצרים, הקובע שמעמדה של תוכנה מוגנת הוא כמעמד כל יצירה ספרותית.

צעד ראשון בנושא הקבילות המשפטית של פלט המחשב נעשה בשנת 1989, בתיקון חוק הוצאה לפועל, התשכ"ז - 1967. נוסף סעיף 79א' הקובע שמסמך שהופק באמצעות מערכת ממוכנת בלשכת הוצאה לפועל ישמש, לכאורה, ראיה לנכונות האמור בו.

בהמשך יתואר המצב במשפטי בישראל, בתחום הגנת תוכנה ובתחום "עבירות מחשב". המונח "עבירות מחשב" הושם במרכאות, כי כפי שיתברר בהמשך, לא כל התנהגות שאינה רצויה לחברה היא בגדר עבירה, במצב החוק הנוכחי.

הגנת תוכנה

כדי ליצור מוצר תוכנה יש להשקיע משאבים רבים. נדרשים זמן לימוד ורכישת מיומנות, מאמץ אינטלקטואלי, שעות עבודה רבות ושימוש בציוד אלקטרוני לצורך התכנות, ניפוי השגיאות והתיעוד. במלים אחרות, לתוכנה יש ערך כלכלי. אין ספק שמחבר התוכנה ובעליה זכאים להגנה משפטית, כדי שהתוכנה לא תועתק ללא רשות וכדי שלא תהיה חופשית לשימוש לכל דכפין. כשם שיש הגנות וזכויות משפטיות לממציא הפטנט ולמחבר היצירה הספרותית והמוסיקלית, כך יש גם להגן על זכויות התוכנה, שאם לא כן, לא תהיה ההשקעה כדאית. לכן, אי הגנה תבלום את פיתוח התוכנה. מובן שהגנה המשפטית היא הגנה משלימה שמצטרפת להגנות הטכניות בתחום אבטחת המידע, כמו סיסמאות, הצפנות, קציני בטיחות, מבקרי ענ"א וכיו"ב.

נושא ההגנה המשפטית לתוכנה הגיע לבית המשפט המחוזי בתל אביב בתיק אזרחי 3021/84, בעניין Apple Computer Inc וידע מחשבים ותוכנה (1982) בע"מ, נגד ניו-קום טכנולוגיות בע"מ. התובעת טענה שהנתבעת מוכרת בישראל מחשבים אישיים תואמי Apple, שמותקנות בהם תוכנות מערכת הפעלה. תוכנות אלו, כך נטען, נכתבו ופותחו במאמץ וכישרון רבים, על ידי עובדי התובעת ולנתבעת אין זכות להעתיק את התוכנות ולשווקן. השאלה המרכזית שעלתה לדיון היתה האם חלים דיני זכויות היוצרים הקיימים בישראל גם על התוכנה. זכות היוצרים היא זכות קניין ערטילאית שקיימת בישראל מכוח פקודה בריטית שנחקקה בבריטניה ב-1911 והוחלה על פלסטינה-א"י ב-1924, שלפיה מוגנת יצירה מקורית ספרותית, דרמטית, מוסיקלית ואמנותית. הגדרת יצירה ספרותית כוללת מפות, תרשימים, תוכניות, טבלאות וליקוטים.

כבוד השופט חאג'-יחיא קבע, שיש לפרש בליברליות ובאופן מרחיב את החוק ושיש להחיל את הגדרת היצירה הספרותית גם על יצירות חדשות, בהתאם להתפתחות הטכנולוגית, גם אם המחוקק לא התייחס אליהן ואף אם לא היו קיימות בזמן החקיקה. באשר לתוכנה, נקבע בפסק הדין: "תוכנת מחשב שהיא פרי רוחו של האדם היוצר וכותב אותה, היא יצירה ספרותית, כמשמעותה בהגדרת החוק, בהיותה ממלאת אחרי התכונות והקריטריונים של יצירה ספרותית, וכי תוכנת מחשב, הן ב-Source Code והן ב-Object Code, בין שהיא כתובה ומודפסת בתקליטונים ובין שהיא אגורה ב-ROM, היא יצירה ספרותית מוגנת על ידי החוק". בית המשפט אימץ בהחלטה זו את הקו שנקטו מדינות מערביות רבות, כמו ארצות הברית, קנדה, אוסטרליה, דרום אפריקה, בריטניה ועוד.

בשנת 1988 חוקקה הכנסת את התיקון לפקודת זכות יוצרים (מספר 5) ובו נקבע באופן מפורש ש"לעניין זכות יוצרים, דין תוכנה של מחשב כדין יצירה ספרותית כמשמעותה בחוק זכות יוצרים 1911". לכן, התוכנה מוגנת היום על ידי הענף המשפטי שנקרא זכויות יוצרים. זכות היוצרים קיימת מאז היווצרות היצירה והיא מונעת העתקה, מכירה, שיווק, הפצה והשכרה ללא רשות הבעלים, עד תום 50 שנה לאחר מות הסופר. זכות היוצרים מקנה הגנה על המוצר הסופי שבתוכו מתמקד רעיון, אך לא על הרעיון עצמו.

בפס"ד ע"א 15/81 של בית המשפט העליון בעניין גולדנברג נ. בנט נאמר: "רעיונות הם נחלת הכלל והוא הדין לעניין הסגנון, אולם מאידך גיסא חלה זכות היוצרים על אופן הביטוי של הרעיונות". פסק דין זה דן במחזמר, אך אם ניישם את הדברים על תוכנה, נמצא שאין הגנה לנושא התוכנה אלא לקידוד. אם יכתוב פלוני תוכנה לניפוק מלאי אוטומטי למשל, הוא לא יוכל לתבוע אלמוני שכתב אף הוא תוכנה לאותו נושא. לעומת זאת, אם העתיק אלמוני קטעים מהקידוד של פלוני, תקום עילת התביעה. כידוע, מושקעים גם מאמץ ועמל רבים בשלבים הקודמים לקידוד, כמו למשל, שלב הגדרת הדרישות ושלב התכנון. ההשקעה בשלבים אלה גדולה לעתים מההשקעה בקידוד עצמו. קיימים כבר תקדימים לכך שגם התוצרים של שלבים אלה, כמו תרשימי זרימה, מבני נתונים ותיעוד יהיו מוגנים, גם אם התכנות על פי תוצרים אלה נעשה ללא העתקה ובאופן עצמאי. כמו כן, יש להניח שבמקרים שבהם הושקעה יצירתיות, כמו במבנה מסך והתנועה על פניו (כמו למשל, במשחקי מחשב) תינתן הגנה למסך גם אם הקידוד ליצירתו יהיה שונה, או בשפת תכנות אחרת.

קו הגבול בין רעיון לאופן ביטויו אינו מובן מאליו ובכל מקרה ידון

בית המשפט לגופו ויקבע, בהתאם לנסיבות, את מידת הדמיון ואם היתה העתקה. לצורך קבלת ההחלטה נעזר בית המשפט במקרים רבים בחוות דעת של מומחים מקצועיים, שבדקו את התוכנות שבמחלוקת. כמובן שכאשר מדובר בהעתקה מלאה של תוכנה, הבדיקה מאוד פשוטה והתובע זוכה בתביעתו.
התרופות להן זכאי בעל התוכנה במקרה של הפרת זכותו, הן צו מניעה, שמונע מהמפר להמשיך ולבצע העתקה, הפצה וכיו"ב, וכן פיצויים בגין אותם נזקים שנגרמו לבעל הזכות. כך למשל, אם הפיץ המפר מאה עותקים של התוכנה, וכתוצאה מכך הפסיד בעל הזכות את אותן 100 מכירות, יוכל המפסיד לקבל פיצוי. הפרת זכות היוצרים מהווה גם עבירה פלילית שעונשים חמורים בצידה. בית המשפט מוסמך לגזור מאסר של עד שלוש שנים וכן קנס כספי גבוה. יש לציין שכדי להביא אדם לדין פלילי בגין הפרת זכות יוצרים, על בעל הזכות לתבוע אותו בעצמו בהליך שנקרא "קובלנה פלילית". זהו מצב השונה מרוב העבירות הפליליות, כמו גניבה, התפרצות, רצח וכיו"ב, שבהם התובעת (ומנהלת התביעה) היא המדינה, באמצעות הפרקליטות או המשטרה, בהתאם לשיקול דעתה הבלעדי. כאמור, במקרה של העתקת תוכנה, בעל הזכות הוא המחליט את מי ומתי לתבוע והוא המנהל את פרשת התביעה, לרבות הזמנת העדים, חקירתם והוכחת האשמה.

הדין הישראלי אינו מתנה את ההגנה על תוכנה בצעדים רשמיים כלשהם, אך למרות זאת, מומלץ לציין על כל תוצר את הסימון המקובל (C) או Copyright בתוספת All Rights Reserved ובציון שנת הפרסום ושם בעל הזכות. רצוי שהודעה זו תוקרן על גבי המסכים של התוכנה ותלווה את התיעוד ואת שאר התוצרים הנלווים. יצויין שיש גם אמנות בינלאומיות שמקנות הגנה בין מדינתית לזכות יוצרים. אולם, בכל מקרה של ייצוא תוכנה, יש לבדוק אם חלה אמנה כלשהי על שתי המדינות ואם יש בארץ היעד דרישות פרוצדורליות אחרות שאינן קיימות בישראל.

לסיכום ייאמר שהמערכת המשפטית מקנה היום הגנה מקיפה על זכויות המחבר ובעל התוכנה. בנוסף לעילת התביעה האזרחית והסעדים הנלווים, כמו צו מניעה ופיצויים, קיימת גם אפשרות ההרשעה בפלילים, על העונשים החמורים והסטיגמה שנלווים אליה. קיימים אמנם הכלים המשפטיים הדרושים ויחד עם זאת, על מחבר התוכנה לשקול ולהחליט על הגנת התוכנה גם באמצעים טכנולוגיים כדוגמת הצפנה, סיסמאות, השמדה עצמית וכיו"ב. כאשר עוסקים בתכנות מסוג מסוים (כמו למשל, תוכנות שמיועדות לשימוש במחשבים אישיים) והתוכנה אינה מוגנת היטב מבחינה טכנולוגית, לא יהיה זה מעשי, בדרך כלל, לתבוע את המעתיקים הרבים.

"עבירות מחשב"

המערכת המשפטית מתאימה את עצמה באיטיות להתפתחויות הטכנולוגיות ובינתיים - מתאים הפשע את עצמו במהירות רבה יותר. בסביבה של מחשבים, אנו עדים בתקופתנו למגוון של התנהגויות מזיקות מבחינת האינטרס הציבורי, שעל החברה להגן על עצמה מבפניהן. על המערכת המשפטית לקבוע שהתנהגויות אלו אסורות על פי הדין הפלילי ולהעניש את העוברים על האיסור. חלק ניכר מהתנהגויות אלו הן סוגי פעילות שלא היו קיימים ולא היו אפשריים לפני עידן המחשב ולכן, החוק הקודם לא יכול היה לצפות אותן ולאסור עליהן במפורש. אפשר לחלק התנהגויות אלו לשלוש קבוצות: חבלה פיסית במחשבים, פשע בסיוע טכנולוגיית המחשבים והתנהגות שלילית כלפי תוכנה וקבצי מידע.

1 חבלה פיסית במחשבים

מרכז המחשבים של מוסד שלטוני, תאגיד כלכלי, או ארגון אחר, מסמל במידה רבה את כוח השליטה של אותו גוף או מוסד. מרכזי המחשבים הופכים לעתים ליעד תקיפה של המתנגדים לארגון. ידועים מקרים של התנגדות על רקע פוליטי, תנועות מחאה אזרחיות, מחתרות טירור ולהבדיל - סכסוכי עובדים שהתבצעו בהם חבלות פיסיות, לרבות פיצוץ יחידת המחשב. מהו יחס המשפט לתופעות אלו? אין ספק שהתנהגות כזו אסורה בלא קשר ליעד התקיפה, בין אם הוא מחשב או כל נכס אחר. בסוג עבירות זה אין כל קושי משפטי וסעיפי החוק האוסרים חבלה וגרימת נזק למבנה ולרכוש חלים באותה מידה גם על הפוגעים במחשבים.

2 פשע בסיוע טכנולוגיית המחשבים

המחשוב חדר באופן מסיבי למערכות כלכליות ופיננסיות וכמעט כל תהליך של תזרים מזומנים (כמו למשל, חישוב משכורות, תשלומים לספקים, קצבאות וגמלאות, העברות בין בנקאיות, מערכות מיסוי) נשלט ומבוצע על ידי מחשב ומערכת מידע. כניסת המחשב לתהליכים אלה יוצרת אפשרות רבות לפשיעה, כמו גניבה, מעילה או מירמה. כמות הנתונים הגדולה שבמאגרי הנתונים, העיבוד המהיר וחוסר הצורך בפעולה פיסית נגד אנשים ורכוש, יוצרים פיתוי גדול לעבריינים, למרות שנדרשת מהם רמה גבוהה של תחכום.

קיימות דוגמאות רבות להטיית כספים לחשבונות פיקטיביים, ליצירת רשומות של ספקים דמיוניים, להעברת שאריות של פעולות חשבונאיות לחשבונות חיצוניים ולמקרי גניבה והונאה שפגעו בבנקים, בחברות ביטוח, במפעלי תעשייה, ביחידות ממשלתיות וכד'. פשעים אלה נעשים, בדרך כלל, על ידי שינויים לא מורשים בתוכנה שמפעילה את המערכת, דיווח של נתונים כוזבים; או התחברות לא מורשית לרשת תקשורת.

גם בסוג זה של התנהגות אין, באופן עקרוני, קושי משפטי. טכנולוגיית המחשבים משמשת במקרים אלה רק אמצעי לפשע בדומה לכל כלי פשע אחר. מתקיימים כאן כל היסודות של עבירות גניבה, מירמה ודומיהן, אך במקום נטילה פיסית של שטרות כסף מהקופה, שימוש בעט לצורך זיוף ספרים, או פעולה אלימה, נעשה כאן שימוש בתוכנה ו/או במחשב. מטרת ההתנהגות ותוצאותיה הסופיות היא גניבה, וזו אסורה על פי החוק הקיים, ללא קשר לאמצעי שבו השתמש העבריין. קיימת לכך, אם כן, תשובה בחוק: ההתנהגות אסורה והעבריין צפוי לעונש. אולם יש לזכור שבשל היעדר של פעילות פיסית ובשל התחכום של העבירה, קיים, לעתים קרובות, קושי רב באיתור העבירה וגם כאשר היא מתגלה קיימים קשיים נוספים בחשיפת אופן הביצוע, גילוי העבריין, השגת הראיות המרשיעות והוכחת האשמה בבית המשפט.

הנזקים הפוטנציאליים הרבים שעלולים להיגרם באמצעות מערכות המידע והקושי לאתר ולהעניש את העבריינים מדגישים את החשיבות הגדולה של אבטחת מערכות המידע באמצעים טכנולוגיים, כדי למנוע, ככל האפשר, את הפגיעות. במלים אחרות, אבטחת המידע, הכנסת אמצעי ביקורת למערכות המחשוב, הגנה פיסית, הצפנה, סיסמאות, מידור וכיו"ב, לוקחים חלק חשוב מאוד במניעת העבירות, בנוסף לאיסורים ולענישה שמספקת המערכת

המשפטית.

3 התנהגות שלילית כלפי תוכנה וקבצי מידע

התוכנה והמידע האגור בקבצים הם התוצרים החדשים שיצר המחשב. התוכנה והמידע, כאותות אלקטרוניים בלתי מוחשיים, הם כלים חשובים מאוד בעידן המודרני, אך עם זאת, הם גם יעד להתנהגויות לא רצויות ומזיקות, שיש להתגונן מפניהן. להלן כמה דוגמאות: העתקת מידע כמו נתוני מאזן של ארגון מקובץ מחשב; מחיקת קבצים; שינוי לא מוסמך של נתונים; החדרת וירוסים; גילוי והדלפה של מידע על ידי עובדים בארגון ועוד.

אין ספק שהתנהגויות אלו והדומות להן מזיקות וראויות לגינוי ולכן, יש לאסור אותן בחוק. אולם, מכיוון שמדובר בהתנהגויות חדשות, המכוונות כלפי תוצרים חדשים, אין אפשרות, במקרים רבים, להכפיף התנהגויות אלו לחקיקה הקיימת. עיקרון משפטי חשוב קובע שעל החוק לקבוע במפורש איזו התנהגות אסורה, וכל מה שלא נאסר במפורש נחשב כמותר. בית המשפט אינו רשאי לקבוע שהתנהגות מסוימת היא עבירה, כל עוד לא נקבע הדבר בחוק, גם אם אותה התנהגות אינה מוסרית, או אינה צודקת. יתר על כן, על מנת להרשיע נאשם, יש להוכיח שקוימו כל יסודות העבירה כלשונן. לדוגמה, עבירת הגניבה, לפי הגדרתה בחוק העונשין, היא לקיחת דבר בלא הסכמת הבעלים, מתוך כוונה של שלילה לצמיתות. על מנת להרשיע אדם בגניבת חשמל באמצעות התחברות למונה של שכנו, היה על המחוקק להוסיף לחוק סעיף מיוחד, מכיוון שחשמל אינו ניתן לנטילה. כדי להרשיע גנבי רכב, נוצר סעיף מיוחד בחוק של שימוש ברכב ללא רשות, מכיוון שלא מתקיים כאן, בדרך כלל, היסוד של כוונת שלילה לצמיתות. הדוגמאות שהוזכרו ממחישות את החשיבות של ההגדרה המדויקת של כל עבירה.

כל עוד אין בחוק העונשין הגדרה של "עבירות מחשב", שיעדן תוכנה ומידע, סוגים רבים של התנהגות פסולה אינם אסורים על פי החוק עד עצם היום הזה. בכל מקרה יש לבדוק אם ההתנהגות המסוימת ממלאת אחת כל יסודותיה של עבירה קיימת. יש לבדוק למשל, אם בחדירה בלתי מורשית מסוימת למאגר באמצעות תקשורת, קיימים כל מרכיביה של עבירת השגת גבול, עבירת מירמה, או התחזות לאחר; אם שינוי נתון על גבי מדיה מגנטית ממלא את דרישות עבירת הזיוף; אם מחיקת מידע מעל גבי דיסק תחשב כפגיעה בנכס. התשובות לשאלות אלו והדומות להן, תהיה במקרים רבים שלילית, וזו הסיבה העיקרית לכך שעד היום היו מעט מאוד תביעות פליליות, ועוד פחות הרשעות בדין, בתחומים אלה.

יש, לפיכך, צורך בחקיקה מיוחדת שתתייחס להתנהגויות הפסולות ותגדיר אותן במפורש כעבירות פליליות שעונש בצידן. החקיקה המיוחדת יכולה להעשות כתיקונים לחוק העונשין, או בפרק בחוק מחשבים מקיף. כל עוד לא התייחס המחוקק באופן מפורש להתנהגויות פסולות כלפי תוכנה ומידע, ירבו המקרים שבהם לא תהיה בידי החברה אפשרות להרשיע ולהעניש על עבירות כאלו, למרות ההסכמה הכללית שהתנהגויות אלו אינן מוסריות והן עלולות לגרום נזק רב לציבור.

חוק אבטחת הפרטיות ודרכי יישומו

הבהרות איל"א

הנהלת איל"א החליטה על הקמת וועדה שתפקידה להכין מסמך שיסביר ויבהיר את דרישות החוק ודרכי יישומו. המסמך פורסם באוגוסט 1987.
מודגש שהסברים אלה לחוק ולתקנות הם לצורך התמצאות בלבד, אין בהם כדי לבוא במקום החוק והתקנות והם אינם משמשים כפרשנות לחוק.
הערת המו"ל: בנספח זה השתמשנו בקטעים מן המסמך שהוכן ע"י הוועדה של איל"א. אנו מודים להנהלת איל"א על הרשות להשתמש בחומר זה.

פרק א - מבוא כללי

1. מבוא

בארצות שונות קיימים חוקים לאבטחת זכויות הפרט במערכות מידע ממוחשבות. הטיפול בנושא חדש יחסית, החל בראשית שנות השבעים, כאשר השימוש במחשבים כבר הקיף חלקים ניכרים מחיי היום יום של הפרט. במרבית הארצות לא קיימת הגדרה ברורה של פרטיות. החוקים הקיימים דנים באיסורים ספציפיים, כמו איסור פתיחת דברי דואר וסודיות קשר טלפון וטלגרף. בשנת 1981 התקבל בארץ חוק הגנת הפרטיות, במסגרתו קיימת התייחסות להגנה על הפרטיות במאגרי מידע ממוחשבים.

2. עקרונות החוק

1. קיומו של מאגר מידע ממוחשב שיש בו נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דיעותיו ואמונתו, לא יהא חסוי. החוק ומסמך זה דנים רק במאגרי מידע אלה.
2. חייבת להיות דרך לפרט לדעת איזה מידע אודותיו רשום בקבצים ולאילו מטרות הוא נועד.
3. חייבת להיות דרך לפרט למנוע שימוש במידע למטרות אחרות מאלו שלשמן נאסף.
4. חייבת להיות דרך לפרט לתקן מידע שגוי אודותיו או לבטלו.
5. ארגון המחזיק נתונים על פרטים חייב להגן על המידע שברשותו מפני דליפה, שימוש לא הוגן או השמדה.

פרק ב - על מי חל החוק?

1. כללי

א. חוק הגנת הפרטיות, התשמ"א-1981, בא לאסור פגיעה בפרטיות הזולת. עיסוקנו הוא באותו חלק של החוק הדן בהגנה על הפרטיות במאגרי מידע.
ב. כאשר קיים ספק לגבי פרשנותה או היקף תחולתה של הוראה מסויימת, ניתן לפנות לרשם מאגרי המידע במשרד המשפטים.
ג. הפרת הוראותיו של החוק היא עבירה פלילית שדינה מאסר עד שנה וכן יכולה לגרור תביעת נזיקין אזרחית.

2. מאגר מידע מהו?

א. מאגר מידע מוגדר בחוק כ"מרכז להחסנת מידע באמצעות מערכת עיבוד נתונים אוטומטית". "מידע" מוגדר כ"נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו".
מדובר כאן ב"אדם" ולא בתאגיד, שכן מטרת החוק היא להגן על הפרטיות ואין הוא בא להגן על אינטרסים כלכליים, מסחריים וכיו"ב, חשובים וראויים להגנה ככל שיהיו. ככל שאדם עלול להיפגע יותר מגילוי ברבים של המידע אודותיו, כך עולה גם רמת רגישות המידע ועימה רמת האבטחה שיש לנקוט לשמירתו.

החוק מקיף כל מה שקשור באדם. כמעט כל מאגר מידע שמצויים בו פרטים על אנשים, ייכנס למסגרת של "מאגר מידע" כמוגדר בחוק. כך, למשל, יכול המאגר לכלול נושאים כמו כח אדם ושכר; אוכלוסין; מקצועות ועיסוקים; שיווק; מחקר וסקרים; ספקים; רפואה; מקרקעין; חינוך; פרסומים; גביה; הנהלת חשבונות וכיו"ב ובלבד, שיש בהם "מידע" על אנשים שניתן לזהותם, כפרטים.

ב. ל"מידע" שהחוק חל עליו, שתי רמות: "מידע" רגיל, ו"מידע מוגבל" שהוא:
1) מידע על מצב בריאותו של אדם;
2) מידע במאגר מידע של רשות בטחון;
3) מידע שבטחון המדינה, יחסי החוץ שלה או הוראות חיקוק מחייבים שלא לגלותו לאדם שהמידע הוא אודותיו;
4) מידע אחר ששר המשפטים קבע בצו כי הוא מוגבל; לגבי מידע כזה חלים כללים מיוחדים.

3. מה מוטל על מי?

החוק קובע לגבי מי שיש לו זיקה למאגרי מידע, חובות ואיסורים מסוימים, כגון:

א. איסור ניהול מאגר לא רשום

אסור לנהל או להחזיק מאגר מידע אשר בו מנוהל מידע כהגדרתו בחוק זה, שאינו רשום בפנקס מאגרי המידע. הרוצה לנהל או להחזיק מאגר חייב לרשמו.

ב. חובת הרישום

על הבעלים או המחזיק של מאגר מידע, לרשום אותו אצל רשם מאגרי המידע במשרד המשפטים ולהודיע לרשם על כל שינוי בפרט מהפרטים הטעונים רישום. רשימת המאגרים ופרטיהם פתוחה לעיונו של הציבור.

ג. סמכויות הרשם

על כל הנוגע בדבר למסור לרשם מאגרי המידע, לפי דרישתו, ידיעות ותעודות המתייחסות למאגר המידע. הרשם רשאי להיכנס למשרדי מאגר מידע ומתקניו, כדי לחפש ולתפוס כל דבר, כדי להבטיח ביצוע החוק או כדי למנוע עבירה.

ד. השימוש במידע

אסור לאדם להשתמש במידע שבמאגר המידע, אלא למטרה שלשמה הוקם המאגר או למטרה שלשמה נועד המידע. מסירת מידע מותרת, בין גופים ציבוריים, במקרים ובתנאים שנקבעו בחוק ובתקנות.

ה. סודיות

אסור לאדם שהגיע אליו מידע בתוקף תפקידו במאגר מידע, לגלותו לאחר, אלא לצורך ביצוע עבודתו או לצורך ביצוע החוק או על פי צו בית משפט בקשר להליך משפטי.

ו. חובת מבקש מידע

כאשר פונים לאדם ומבקשים ממנו מידע לשם החזקתו או שימוש בו במאגר מידע, יש להודיע לו:
1) אם חלה עליו חובה חוקית למסור את המידע, או שהדבר תלוי ברצונו או בהסכמתו;
2) מהי המטרה שלשמה מבוקש המידע;
3) למי יימסר המידע ומה מטרות המסירה.

ז. זכות עיון במידע

לכל אדם זכות עיון במידע שעליו, המוחזק במאגר מידע.
זכות העיון אינה קיימת לגבי מאגרי מידע מסוימים:
1) מאגר מידע של רשות בטחון, דהיינו - משטרת ישראל, המשטרה הצבאית, אגף המודיעין במטכ"ל, שב"כ והמוסד.
2) מאגר מידע של רשויות המס;
3) כשהמידע נוגע לבטחון המדינה או ליחסי החוץ שלה;
4) כשהוראת חיקוק מחייבת לא לגלות לאדם מידע אודותיו.

הוראה מיוחדת קיימת לגבי הצגת מידע המתייחס למצב בריאותו של אדם. מידע כזה יוצג רק באמצעות רופא, אשר רשאי למנוע מטעמים רפואיים מידע מהמבקש.
על סירוב בעל מאגר מידע לאפשר עיון, כאמור, רשאי מבקש המידע לערער.

ח. תיקון מידע

אדם שעיין במידע שעליו ומצא כי אינו נכון, שלם, ברור או מעודכן, רשאי לפנות לבעל המאגר, או למחזיק המאגר, בבקשה לתקן את המידע או למחקו.

על בעל המאגר לבצע את השינויים המבוקשים וגם להודיע עליהם לכל מי שקיבל ממנו את המידע. אם בעל המאגר מסרב מסיבה כלשהי לעשות כן, עליו להודיע על כך למבקש והמבקש רשאי לערער על כך בפני בית משפט השלום.

ט. **אמצעי אבטחה**

על מנהל המאגר לנקוט אמצעי אבטחה כדי לשמור על שלמותו של המידע שבמאגר וכדי למנוע חדירת גורמים בלתי מוסמכים אליו.

פרק ג - מיהו מנהל המאגר ומה המידע הכלול במאגר?

1. כללי

עיקר ההוראות הנוגעות לניהול מאגר מידע, מצוי ב"תקנות הגנת הפרטיות" (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ז-1986 (ק"ת התשמ"ו, עמ' 858).

2. מיהו "מנהל המאגר"

"מנהל מאגר" הוא המנהל הכללי של הגוף שבבעלותו מצוי מאגר מידע, או מי שהוא הסמיכו לענין זה. הכוונה היתה להבטיח הקצאת האמצעים התקציביים הנדרשים. על הסמכת מנהל מאגר מידע יש להודיע בכתב לרשם מאגרי המידע, לידיעת הכלל.

3. אחריות מנהל מאגר

א. מנהל מאגר אחראי לנקיטת האמצעים הדרושים לשם קיום תקנות אלו, בהתאם לנסיבות השימוש במאגר המידע שעליו הוא מופקד. משמעות הוראה זו היא כי היקף השימוש בכל אחד מהאמצעים מותנה בכל הנסיבות של השימוש במאגר המידע ובמאפיינים של אותה מערכת.

ב. מנהל המאגר אחראי לאבטחת המידע, כלומר - להגנתו מפני שינוי, השמדה או חשיפה, במאגר המידע שעליו הוא מופקד ובכלל זה בתחומים אלה:

1) קיום הגנה פיסית על מערכת עיבוד הנתונים האוטומטית (להלן - המערכת) ועל תשתיתה, לרבות מבנה, אמצעי תקשורת, מסופים ותשתית חשמלית, מפני סיכונים סביבתיים ופגיעות;

2) קביעת סדרי ניהול של מאגר מידע וכללים להרשאת גישה למידע, לאיסוף, לסימון, לאימות, לעיבוד ולהפצה של המידע, הכל בהתאם להוראות החוק והתקנות. סדרים וכללים, יחולו, כאמור, גם על נותן שירותים חיצוני לגוף שבבעלותו מאגר המידע;

3) קיום הוראות תפעול של המערכת תוך אבטחת המידע ושמירה על שלמות המידע. החוק קבע כי לצורך ענייננו, שלמות המידע כוללת: זהות הנתונים במאגר למקור ממנו נשאבו; אי מסירתו ואי השמדתו ללא הרשאה.

4) נקיטת אמצעי אבטחה סבירים, בהתאם לרמת רגישות המידע, שימנעו חדירה מכוונת או מקרית למערכת אל מעבר לתחומי המידע שאושרו למשתמש; רמת רגישות המידע תלויה במידת הפגיעה שאדם עלול להיפגע, אם יתגלה ברבים המידע אודותיו.

5) קביעת סדרי בקרה לגילוי פגיעות בשלמות המידע ותיקון ליקויים.

ג. מנהל המאגר הוא האחראי להפעלת הכללים המיוחדים החלים על מאגר מידע המכיל "מידע מוגבל" ועליו לעשות כן בהתאם לנסיבות.

פרק ד - העברת מידע בין גופים ציבוריים

1. כללי

א. חוק הגנת הפרטיות והתקנות שהותקנו על פיו, קובעים הוראות מיוחדות לגבי העברת מידע בין גופים ציבוריים. גוף ציבורי הינו:

1) משרדי הממשלה ומוסדות מדינה אחרים, רשות מקומית וגוף אחר הממלא תפקידים ציבוריים על פי דין, כמו: ועדת חקירה ממלכתית. מעמד מיוחד נקבע בחוק ל"רשות בטחון": משטרת ישראל, המשטרה הצבאית, אגף המודיעין במטכ"ל, שב"כ והמוסד למודיעין ולתפקידים מיוחדים.

2) גופי אחרים שנקבעו ע"י שר המשפטים באישור ועדת החוקה, חוק ומשפט של הכנסת, תוך ציון סוגי המידע והידיעות שהגוף רשאי למסור ולקבל:
א) בית חולים - ידיעות על מצב בריאותו של אדם לצורך הטיפול בו.
ב) קופת חולים - ידיעות על מצב בריאותו של אדם לצורך הטיפול בו.
ג) מוסד להשכלה גבוהה - פרטים אישיים לצרכי מחקר.

ב. ההוראות הנוגעות למסירת מידע בין גופים ציבוריים מציינות, כי כל ידיעה על ענין פרטי של אדם הינה בגדר מידע לצורך הדיון בהעברת מידע.

2. כללים להעברת המידע

א. בד"כ אסור לגוף ציבורי למסור מידע, אלא במקרים הבאים:
1) המידע כבר פורסם ברבים על פי סמכות כדין;
2) המידע הועמד לעיון הרבים על פי סמכות כדין (למשל, פנקס הבוחרים);
3) האדם שהמידע מתייחס אליו נתן את הסכמתו למסירת המידע.

ב. איסור זה אינו חל על "רשות בטחון". זו רשאית הן לקבל מידע והן למסרו.

ג. על אף האיסור הכללי, מותר בכ"ז למסור מידע בין גופים ציבוריים, בתנאי:
1) שהדבר לא נאסר בחיקוק או בעקרונות של אתיקה מקצועית;
2) שאין מדובר במידע אשר ניתן בתנאי שהוא לא יימסר לאחר.

ד. הסדר מיוחד נקבע בפקודת התעבורה לגבי מאגר המידע של רשות הרישוי.

פרק ה - טיפול במידע מוגבל

1. מידע מוגבל מהו?

א. "מידע" כולל סוגים שונים של מידע הקשורים בפרט.

ב. מנהל מאגר המידע צריך לנקוט באמצעי אבטחה סבירים בהתאם "לרמת רגישות המידע". רמות הרגישות לא נקבעו, אולם לפנינו לפחות שתי רמות מידע והן:
1) "מידע כללי"; 2) "מידע מוגבל".

ג. "מידע מוגבל" הוא כל אחד מאלה:
1) מידע על מצב בריאותו של אדם.
2) מידע המצוי במאגר של רשות בטחון ושל רשות מס.
3) מידע "סודי" (הקשור ברשויות הבטחון).

2. כללים לטיפול במידע מוגבל

א. מנהל המאגר חייב להפעיל את הכללים שבנידון בהתאם לנסיבות השימוש.

ב. למאגר מידע המכיל מידע מוגבל חייב להיות קובץ נהלים המפרט:
1) את אמצעי האבטחה והבקרה על הטיפול הפיסי באמצעי האחסון של המידע.
2) פרק מיוחד לטיפול במידע בידי נותן שירותים חיצוניים בתחומי:
א) הקלדה; ב) עיבוד נתונים; ג) הפצת דוחות והובלת קבצים.

ג. השאלה של אמצעי רישום מגנטי המכיל מידע מחייבת רישום בתעודת משלוח (עם אישור מצד המקבל) וסימון על האמצעי עצמו.

ד. אמצעים שסומנו כאמור יאוחסנו במדור סגור ועותקי גיבוי שלהם יימצאו מחוץ למתקן הראשי.

ה. קבצים נתיקים ותדפיסי מחשב המופקים עבור גוף ציבורי יופקו בלווית כתובת בולטת בכל עמוד, בה ייאמר: "מכיל מידע מוגן לפי חוק הגנת הפרטיות - המוסרו שלא כדין עובר עבירה".

ו. אמצעי רישום מגנטיים ופלט מחשב כתוב של הליכי ביניים יפונו מיד לביעור במגרסה או יימחקו.

ז. מנהל המאגר ינהל רישום מעודכן של: המשתמשים במידע מוגבל; הרשאות גישה; פירוט קוד גישה וסוגי פעולות המותרים למשתמשים (סיסמאות); יומן אירועים חריגים (פרטי זיהוי של הפונה; סוג השאילתה; הרשומות שהופקו).

פרק ו - מנהל המאגר

1. מיהו מנהל המאגר?

א. החוק קובע שהמנהל הכללי הינו מנהל המאגר, או מי שהוא הסמיכו לענין זה. בקרב ארגונים רבים ממנים אחראי/מנהל המחשב בארגון כמנהל המאגר.

ב. יש לשקול מינוי אדם בכיר בארגון (מנכ"ל או אחד מסגניו) ולא את מנהל יחידת המחשב או האחראי למחשב בארגון, מהסיבות הבאות:
1) המידע הינו משאב הארגון ולא משאב מנהל יחידת המחשב.
2) ניגוד אינטרסים בין דרישות מקצועיות וידע מקצועי לבין הצורך להגן על מאגרי המידע.
3) אין לו בד"כ הסמכות בתוך הארגון ליישם את דרישות החוק להן הוסמך.
4) אין לו בד"כ היכולת והאמצעים לבצע את המוטל עליו במסגרת החוק.

2. דרישות מנהל המאגר מהארגון

על מנת לעמוד בדרישות החוק, דרושים למנהל המידע הדברים הבאים:

א. מינוי בכתב של המנכ"ל.
ב. אישור של ההנהלה לכל הפעולות שייעשו במסגרת החוק.
ג. אישור ההנהלה לתכנית אבטחת המידע, תוך פירוט החלקים שהוחלט לא לבצעם.
ד. דרישות תקציב בסעיף נפרד בספר התקציב ובמידה ולא יאושרו הסכומים הנדרשים יש לקבל על כך החלטת ההנהלה.
ה. זכות לייעוץ משפטי.
ו. הזמנת גורם חיצוני מקצועי (או ביקורת פנימית) לצורך בדיקת התארגנות ליישום התקנות במסגרת הארגון.

פרק ז - נותני שירותים חיצוניים וחברות בת

1. נותני שירותים חיצוניים

א. תקנות הגנת הפרטיות קובעות סדרי ניהול של מאגר מידע וכללים להרשאת גישה ומידע, לאיסוף, לסימון, לאימות, לעיבוד ולהפצה של המידע, הכל בהתאם להוראות החוק והתקנות; סדרים וכללים יחולו, כאמור, גם על נותן שירותים חיצוני לגוף שבבעלותו מאגר המידע.

ב. מומלץ לאתר את אוכלוסית נותני השירותים החיצוניים עפ"י שתי קבוצות:
1) נותני שירותים המחזיקים במחשבים שלהם מידע או נתונים של בעל המאגר, להלן "לשכות שירות".
2) נותני שירותים הפועלים על מידע או נתונים שנמצאים במחשבי בעל המאגר, להלן "קבלנים חיצוניים".

2. חברות בנות

א. כל גוף שבידו מאגר מידע, אחראי לקיום החוק והתקנות בכל הנוגע למאגר המידע שלו, בין אם הוא "חברת אם" או "חברת בת". בקונצרנים מסוימים קיימים מצבים בהם החברה הראשית בקונצרן, אשר ברשותה אמצעי המיחשוב, מעבדת מידע או מספקת שירותי מידע לחברות בנות בקבוצה.

ב. במקרים אלה מומלץ לנקוט בפעולות הבאות:
1) כל חברה בקונצרן בעלת מאגר מידע, תמנה מנהל מאגר מידע משלה.
2) החברה שברשותה אמצעי המיחשוב, תנקוט בכל האמצעים הנדרשים עפ"י חוק. עליה לנקוט בכל האמצעים הדרושים בכדי להפריד את פריטי המידע של כל חברת בת מפריטי המידע שלה עצמה או של חברות בנות אחרות בקונצרן. יש לוודא שלנציגי חברת הבת תתאפשר גישה אך ורק לנתונים השייכים לה.

מוספים

להלן שלושה מוספים טכניים בנושאים הבאים:
- נהלים,
- אבטחת תוכנה,
- אבטחה פיסית

מוסף א - נהלים

1. כללי

א. קיימים נהלים המיועדים לסייע ביישום החוק והתקנות לשמירת הפרטיות. רשימת הנהלים הינה כללית וישימה בכל מערכת מחשב. מתוכה יש לבחור את הנהלים המתאימים ליישום, בהתאם לסוגי המידע, היקף המתקן ושיקולים אחרים.

ב. הנהלים מחולקים לארבע קבוצות עיקריות:
1) נהלים המיועדים להגדרת המודעות לחוק הגנת הפרטיות בארגון.
2) נהלי אבטחה לוגית.
3) נהלי אבטחה פיסית.
4) נהלי טיפול בכח אדם.

(רשימת נהלים מפורטת ניתנת במסמך של איל"א).

מוסף ב - אבטחת תוכנה

1. כללי

א. אבטחה בתוכנה הינה תת-מערכת האבטחה הכוללת את הפיקוח המתבצע על ידי המערכת הממוחשבת. אבטחה בתוכנה כוללת את הכלים:
- לבקרת גישה,
- לניהול יומן אירועים,
- להצפנת נתונים.

2. בקרת גישה

בקרת הגישה למידע במערכות ממוחשבות הכוללות מאגרי מידע נובעת מדרישות הקיימות בחוק.

א. מידע כללי
1) קביעת סדרי הניהול של מאגרי המידע וכללים להרשאת גישה למידע - תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו והעברת מידע בין גופים ציבוריים).
2) "נקיטת אמצעי אבטחה סבירים בהתאם לרמת רגישות המידע, שימנעו חדירה מכוונת או מקרית למערכת אל מעבר לתחומי המידע שאושרו למשתמש".

ב. מידע מוגבל
1) "מנהל המאגר ינהל רישום מעודכן של הרשאות הגישה אשר יכיל שמות ופרטי זיהוי של עובדי המערכת והמשתמשים המורשים גלשת למידע האגור במערכת, פירוט קוד הגישה וסוגי הפעילות המותרים למשתמשים ...".
2) בתקנות ניתנות הנחיות מפורטות יותר של הדרך לביצוע בקרת הגישה:
"...סיסמאות הגישה יוחלפו לעיתים בלתי קבועות, אך לא פחות מאשר אחת לששה חודשים, בעת החלפת עובדים". "יומן אירועים חריגים... לגבי אירוע חריג יירשמו ביומן פרטי הזיהוי של הפונה, סוג השאילתה, הרשומות או סוגי הרשומות שהופקו בתשובה".

3. בקרת גישה - מהי?

בקרת גישה למידע כוללת שיטות לזיהוי הפונה למערכת (כדי לבדוק אם הוא משתמש חוקי) ושיטות לבקרת רמת ההרשאה של הפונה. בקרת הגישה למידע רגיל ולמידע מוגבל מבוססת על אותן שיטות כאשר ההבחנה היא במידת חומרתן של הבקרות.

א. **זיהוי:** זיהוי הוא התהליך שבאמצעותו קובעת מערכת האבטחה שהמשתמש, המשימה והאביזרים במערכת (מחשבים, מסופים) ידועים לה. הבחינה לזיהוי תיערך בכל יצירת קשר מהמערכת. הזיהוי חייב להיעשות לפני שתינתן ההרשאה לגישה לנתונים. סדר הזיהוי יהיה: המשתמש, האביזרים, המשימה.

ב. **הרשאה:** בקרת ההרשאה היא האבטחה שהמשתמש ניגש למשימות (תכניות) בהתאם לכללים מוגדרים מראש. ההרשאה חשובה במיוחד במאגרי נתונים המשותפים לכמה משתמשים במערכת.

4. ניהול יומן אירועים

א. תהליך של רישום ואיסוף כל נתון הנראה נחוץ על מנת לקיים מעקב על פעילות המערכת ואיתור אירועים חריגים.

ב. הרישום ביומן האירועים יכול להיות מלווה:
- בהודעות בזמן אמיתי לקצין הבטחון.
- בפעילות הגנתית כמו נעילת מסוף לאחר פניות שגויות.
- בהוראות פעולה מתאימות לקצין הבטחון.

ג. המחוקק דרש יומן אירועים רק למאגרי מידע מוגבלים.

5. הצפנת (ערבול) נתונים

אמצעי אבטחה הבא למנוע משתמשים לא מורשים מלהבין את הנתונים בקבצים הוא ההצפנה (ערבול). שיטות ההצפנה מבוססות על אלגוריתמים מתמטיים ההופכים את הנתונים לבלתי קריאים ללא מפתח מתאים. המפתח יכול להיות אישי או קבוצתי, פרטי או ציבורי ומוחלף אחת לתקופה קצובה או אקראית.

6. האמצעים

בקרות הגישה מתבצעות בכל אחד מהאמצעים הבאים:
נהלי בקרות; אמצעים פיסיים; אמצעי תוכנה (פעולות ובקרת גישה המבוצעות על ידי המחשב באמצעות טבלאות פנימיות).

7. תוכנת תקשורת

הרשאת הגישה (לוגית) לתוכנת התקשורת תמודר באמצעות סיסמאות כניסה ומערכת הרשאות פנימית. יש לנהל LOG אשר יאפיין את השינויים שבוצעו בתוכנת התקשורת. גורם מבקר בארגון צריך לבדוק זאת מדי יום.

מוסף ג - אבטחה פיסית ותמיכה בהישרדות מערכות מידע

1. אבטחה פיסית

ניתן לחלק למספר תחומים:

א. הגנה פיסית על חדר מחשב.
ב. הגנה פיסית על מערכות מבוזרות.
ג. הגנה פיסית על תשתית תקשורת ומסופים.
ד. אבטחת מדיה מגנטית.
ה. מצפינים.

2. הגנה פיסית על חדר מחשב

יישום האבטחה הפיסית ותמיכה בהישרדות במתקן המחשב המרכזי צריכים לכלול:

א. מניעת גישה פיסית - מערכת בקרת כניסה ממוחשבת או אנושית.
ב. סיכוני אש - מערכת גילוי עשן וכיבוי אש.
ג. אספקת מתח - לוחות חשמל חיצוניים, אל-פסק, גנרטור - בהתאם לתלות הארגון בעבודה רציפה של המערכת.
ד. הצפות - גילוי הצפות וסדרי ניקוז.
ה. מיזוג אוויר - מד טמפרטורה מירבית ולחות.

3. הגנה פיסית על מערכות מבוזרות
מערכות מבוזרות ואמצעי מיחשוב מקומיים, כדוגמת מחשבי PC, חייבים באבטחה פיסית בהתאם לרגישות המידע והנזק האפשרי לפרט.
אמצעים מומלצים:

א. נעילת החדר.

ב. נעילת המחשב במפתח.

ג. נעילת תקליטונים וסרטים בכספת.

4. הגנה פיסית על תשתית תקשורת ומסופים
קווי תקשורת טלפוניים הינם בבעלות חב' "בזק". הם אינם בשליטת הארגון, מיקומם אינו ידוע, ולכן אינם ניתנים להגנה פיסית. אמצעים שמומלץ לנקוט:

א. שימוש מבוקר ומוגבל ב- Data Scope (ציוד בדיקת קווים).

ב. מניעת גישה לא מבוקרת לאיזור לוחות מיתוג המשמשים להעברת נתונים.

ג. מניעת גישה לא מבוקרת למודמים ומרבבים המאפשרים set-up חיצוני.

ד. נעילת מסופים במפתח.

ה. סגירת הגישה לחדרי מסופים בשעות שאין נוכחות, או ניתוק מרכזי שלהם.

ו. במקרים בהם נעשה שימוש בקווי חיוג לתוך מערכת המחשב, למערכות רגישות ביותר, מומלץ לבצע חיוג חוזר (ידני) לגורם היוזם, וזאת כדי לוודא הימצאות הגורם היוזם במיקום הפיסי אשר אושר מראש.

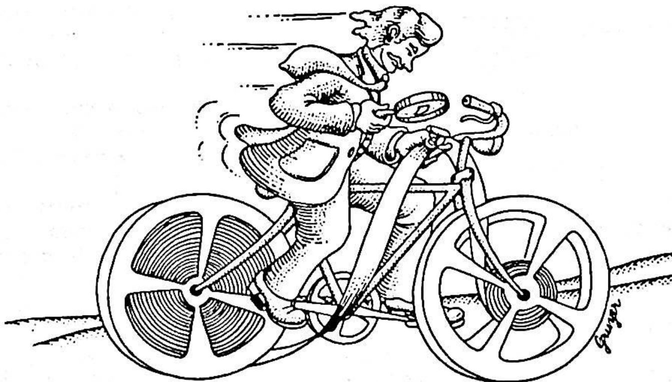
5. אבטחת מצעים מגנטיים
א. יש לנעול תקליטונים, סרטים, קלטות ותקליטים נתיקים וכן להגן עליהם בהימצאם באתר גיבוי מרוחק.

ב. תדפיסים נושאי מידע מוגבל כהגדרתו בחוק, חייבים בשמירה וגריסה.

ג. מצע מגנטי נושא מידע מוגבל - שלא ניתן למחיקה - יש להשמידו.

6. מצפינים
א. אם הארגון משתמש במצפיני חומרה, יש לוודא כי הגישה אליהם תבוקר. ניתן לנעול אותם בארונות או בכל אמצעי הגנה פיסי אחר. מומלץ לתעד גישות הגורמים השונים למכשירי ההצפנה, לצורך בקרה.

ב. יש לזכור לדרוש מספק הציוד אישור להצפנה, כפוף לחוק הצופן.



כללים לאבטחת מידע

על פי המלצות המועצה המייעצת לעניין
אבטחת מידע שבמאגרי מידע

עיקרי ההמלצה

התקנות להגנת הפרטיות נכנסו לתוקפן ביום 11.2.1987. התקנות מתייחסות למאגרי מידע, דהיינו מרכזים לאחסנת מידע באמצעות מערכת עיבוד נתונים אוטומטי, וזאת כאשר המידע הנכלל במאגר הוא כפי שמוגדר בסעיף 7 לחוק. על פי תקנות אלו, על מנהל המאגר לנקוט אמצעי אבטחה כדי לשמור על שלימותו של המידע ולמנוע חדירה של גורמים בלתי מוסמכים אליו.

הערה: ההנחיות ניתנו בצורה כללית והן מדריכות את מנהלי מאגרי המידע לגבי סדר הפעולות שעליהם לנקוט, מתוך התחשבות בעובדה שדרושה תקופת היערכות לקראת יישומן המלא של התקנות. אין מהוראות אלו כדי לגרוע מהוראות כל חקיקה ספציפית החלה לגבי כל מאגר ומאגר.

1. **הכשרה למנהל מאגר מידע**
מן הראוי שמנהל מאגר מידע יעבור הכשרה מתאימה בתחום הצפנה ואבטחת מידע בסביבת מחשבים.

2. **תקציב לביצוע החוק**
יש להקצות למנהל מאגר מידע תקציב מיוחד הדרוש לצורך ביצוע החוק והתקנות עם כניסתו לתפקידו.

3. **בדיקת מהימנות והצהרת סודיות**
3.1 מורשה גישה למידע במאגרי המידע הממוחשבים חייב בבדיקת מהימנות מתאימה, או בהצהרת סודיות לפני קבלת ההרשאה.
3.2 הצהרת הסודיות תכלול התחייבות, לפיה לא יעביר העובד לגורמים בלתי מורשים מידע שיועבר אליו, או ימצא בידיו במסגרת עבודתו בארגון.

4. **מיפוי המידע בארגון**
מנהל מאגר מידע החייב ברישום יבצע מיפוי המידע המצוי בידיו וסיווגו לרמות. יקבעו לפחות שתי רמות סווג: "בלתי מסווג" ו"מסווג".

5. **מיפוי התוכנות בארגון**
מנהל מאגר מידע יבצע מיפוי התוכנות והתוכניות שבאמצעותן ניתן לשלוף, לעדכן, לעבד או לשנות פריטי מידע.

6. **סדרי ניהול**
יקבעו סדרי ניהול וייערכו ההכנות הנדרשות לצורך מתן הגנה ממוחשבת למידע בקבצים ולתוכניות, מתוך הנחה שתקופת היערכות זו לא תעלה על שנה.

7. **מורשי גישה למידע**
7.1 מנהל מאגר יהיה חייב ברישום מורשי מידע בארגון לכל אחת מהרמות שנקבעו במיפוי המידע והתוכניות בארגון.
7.2 פניה של אדם לקבלת מידע שלא בתחום הרשאתו תחייב אישור מוקדם מאת המוסמך לכך.
7.3 עיון או משיכת מידע שלא עפ"י הרשאה מהווה גם עבירה של אתיקה מקצועית, ומחייבת נקיטת אמצעים משמעתיים.

7.4 יוכנו סדרי ניהול המתייחסים למורשי מידע וכן ייערכו ההכנות הנדרשות לצורך מתן הגנה ממוחשבת וזכאות כניסה למורשי מידע.

.8 מיפוי הרשאות גישה לקבלני משנה

8.1 קבלני המשנה יחוייבו באמצעות חוזים או חתימה על הצהרת סודיות לשמירה על מידע מסווג כמפורט לעיל.

8.2 קבלני משנה יחוייבו לכלול בהצעותיהם סעיף המתייחס לנושא הגנת הפרטיות, כפי שיגדירו בעל המאגר.

8.3 יש להקפיד להכניס מחוייבות הקבלן כנ"ל עם כל חידוש חוזה או עריכת חוזה חדש.

.9 סיסמת גישה לקובץ

ייערכו ההכנות הנדרשות לצורך חלוקת ההרשאות וסיסמאות הגישה לקבצים מסווגים בטכניקות ממוחשבות של אבטחת מידע.

.10 סיסמאות למסופים

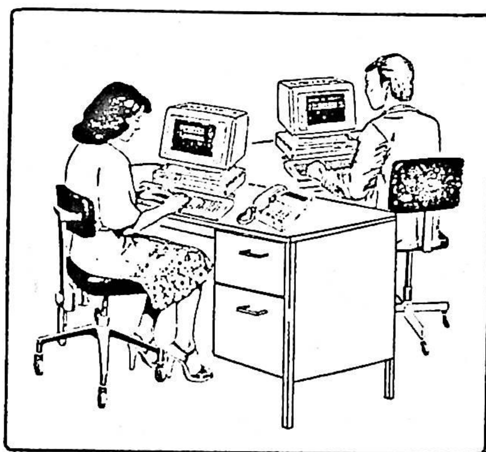
יקבעו סדרי ניהול, הוראות גישה ושימוש במסופים, כמו"כ ייערכו ההכנות הנדרשות לצורך חלוקת צופנים למשתמשי הקצה. לא תורשה גישה למידע, אלא באמצעות צופן.

.11 מערכת התראות ומעקב חריגים

11.1 תופעל מערכת התראות באחריות מנהל המאגר. החריגות יתועדו וישמשו לצורכי הפקת לקחים והסקת מסקנות לקראת קביעת נוהלים קבועים.

11.2 ינוהל מעקב שוטף אחר חריגות. חריגה שתתגלה, יקבל מבצעה התראה. אדם שיבצע 3 חריגות, יוזמן לבירור משמעתי, ותוצאות הבירור ירשמו בתיקו האישי.

11.3 ינוהל רישום החריגים בצורה ידנית או ממוחשבת. מעקב זה ישמש כלי נוסף למשלוח התראות. מומלץ שבדיקת הממצאים ביומן החריגים תתבצע בפרקי זמן שאינם עולים על 30 יום.



חוק הגנת הפרטיות, התשמ"א-1981

(להלן קטעי המבוא של החוק)

פרק א: פגיעה בפרטיות

איסור הפגיעה בפרטיות

1. לא יפגע בפרטיות של זולתו ללא הסכמתו.

פגיעה בפרטיות מהי

2. (1) בילוש או התחקות אחרי אדם, העלולים להטרידו, או הטרדה אחרת;
(2) האזנה האסורה על פי חוק;
(3) צילום אדם כשהוא ברשות היחיד;
(4) פרסום תצלומו של אדם ברבים בנסיבות שבהן עלול הפרסום להשפילו או לבזותו;
(5) העתקת תוכן של מכתב או כתב אחר שלא נועד לפרסום, או שימוש בתוכנו, בלי רשות מאת הנמען או הכותב, והכל אם אין הכתב בעל ערך היסטורי ולא עברו חמש עשרה שנים ממועד כתיבתו;
(6) שימוש בשם אדם, בכינויו, בתמונתו או בקולו, לשם רווח;
(7) הפרה של חובת סודיות שנקבעה בדין לגבי ענייניו הפרטיים של אדם;
(8) הפרה של חובת סודיות לגבי ענייניו הפרטיים של אדם, שנקבעה בהסכם מפורש או משתמע;
(9) שימוש בידיעה על ענייניו הפרטיים של אדם או מסירתה לאחר, שלא למטרה שלשמה נמסרה;
(10) פרסומו או מסירתו של דבר שהושג בדרך פגיעה בפרטיות לפי פסקאות (1) עד (7) או (9);
(11) פרסומו של ענין הנוגע לצנעת חייו האישיים של אדם, או למצב בריאותו, או להתנהגותו ברשות היחיד.

הגדרת מונחים (תיקון תשמ"א)

3. לענין חוק זה -
"אדם" לענין סעיפים 2, 7, 13, 14 ו-25 - למעט תאגיד;
"הסכמה" - במפורש או מכללא;
"פרסום" - כמשמעותו בסעיף 2 לחוק איסור לשון הרע, התשכ"ה - 1965;
"צילום" - לרבות הסרטה.

פגיעה בפרטיות - עוולה אזרחית

4. פגיעה בפרטיות היא עוולה אזרחית, והוראות פקודת הנזיקין [נוסח חדש], יחולו עליה בכפוף להוראות חוק זה.

פגיעה בפרטיות - עבירה

5. הפוגע במזיד בפרטיות זולתו, באחת הדרכים האמורות בסעיף 2(1), (3) עד (7) ו-(9) עד (11), דינו - מאסר שנה.

מעשה של מה בכך

6. לא תהיה זכות לתביעה אזרחית או פלילית לפי חוק זה בשל פגיעה שאין בה ממש.

.... (המשך) ....

תקנות הגנת הפרטיות

(תנאי החזקת מידע ושמירתו
וסדרי העברת מידע בין גופים ציבוריים)
התשמ"ו-1986

(להלן קטעי המבוא של התקנות)

פרק א: פרשנות

הגדרות

1. בתקנות אלה -
"מאגר מידע", "מידע", "מידע עודף", "רשם", "שימוש במידע", "גוף ציבורי" - כמשמעותם בחוק;
"מידע מוגבל" - כל אחד מאלה:
(1) מידע על מצב בריאותו של אדם;
(2) מידע שחלות עליו הוראות סעיף 13(ה)(1), (3) ו-(4) לחוק.
(3) מידע אחר ששר המשפטים קבע בצו כי הוא מוגבל;
"שלמות המידע" זהות הנתונים במאגר מידע למקור ממנו נשאבו, בלא ששונו או נמסרו או הושמדו ללא הרשאה;
"אבטחת מידע" - הגנה על מידע מפני שינוי, השמדה או חשיפה במזיד או במקרה;
"מנהל מאגר" - המנהל הכללי של הגוף שבבעלותו מצוי מאגר מידע, או מי שהוא הסמיכו לענין זה.

פרק ב: הוראות כלליות לניהול מאגר מידע

הודעה על מאגר

2. המנהל הכללי של גוף שבבעלותו מצוי מאגר מידע יודיע לרשם בכתב את שמו של מנהל המאגר וההודעה תירשם בפנקס.

אחריות מנהל מאגר

3. (א) מנהל מאגר אחראי לנקיטת האמצעים הדרושים לשם קיום תקנות אלה, בהתאם לנסיבות השימוש במאגר המידע שעליו הוא מופקד.
(ב) מנהל מאגר אחראי לאבטחת המידע במאגר המידע שעליו הוא מופקד ובכלל זה בתחומים אלה:
(1) קיום הגנה פיסית על מערכת עיבוד הנתונים האוטומטית (להלן - המערכת) ועל תשתיתה לרבות מבנה, אמצעי תקשורת, מוספים ותשתית חשמלית מפני סיכונים סביבתיים ופגיעות;
(2) קביעת סדרי ניהול של מאגר מידע, וכללים הלרשאת גישה למידע, לאיסוף, לסימון, לאימות, לעיבוד ולהפצה של המידע, הכל בהתאם להוראות החוק והתקנות; סדרים וכללים כאמור יחולו גם על נותן שירותים חיצוני לגוף שבבעלותו מאגר המידע;
(3) קיום הוראות תפעול של המערכת תוך אבטחת המידע ושמירה על שלמות המידע;
(4) נקיטת אמצעי אבטחה סבירים, בהתאם לרמת רגישות המידע, שימנעו חדירה מכוונת או מקרית למערכת אל מעבר לתחומי המידע שאושרו למשתמש;
(5) קביעת סדרי בקרה לגילוי פגיעות בשלימות המידע ותיקון ליקויים.

.... (המשך) ....

תזכיר חוק המחשבים

(עבירות, הגנת תוכנה וראיות)
התשמ"ז-1987

(הערה: תזכיר חוק המחשבים כולל מספר נושאים, אשר חלק מהם מתייחס במישרין לנושא ספר זה. נושאים אחרים, כגון "זכויות מחברי תוכנה", "ראיות" ו"שונות" חורגים מנושא הספר והובאו כאן לשם שלימות ההצגה בלבד.)

פרק א': פרשנות

1. הגדרות

בחוק זה -

"מחשב" - מכשיר לקליטת נתונים או לאגירתם, לעיבודם עיבוד אריתמטי או לוגי לפי תכנית ופליטת נתונים, תוצאות, הוראות ביצוע או הפעלה, לרבות ציודו ההיקפי ומערכות תקשורת המחוברות אליו, ולרבות מערכת מחשבים;

"תוכנית" - קבוצת הוראות לשם פעולת מחשב, בין שהיא רשומה בכתב או בצורה אחרת, ובין שהיא מגולמת במכשיר בצורה אלקטרונית, אלקטרומגנטית או אחרת;

"תוכנה" - תוכנית, אפיון תוכנית וחומר עזר לתכנית;

"מידע" - תוצאות של עיבוד נתונים שאותו מחשב הוזן בהם;

"דבר" - לרבות זכויות, טובות הנאה, תוכנה, נתונים במאגר לשימוש במחשב ומידע;

"מעשה" - לרבות מחדל.

פרק ב': עבירות וחדירה למחשב

סימן א': עבירות

2. שיבוש פעולת מחשב

העושה ללא סמכות מעשה במחשב, בחלק מחלקיו או בחלק המיועד לשימוש בהפעלתו, בידעו שהמעשה עשוי למנוע תפעולו התקין או להביא לשיבוש בפעולתו, דינו - מאסר שבע שנים.

3. מניעת שירותי מחשב

(א) העושה ללא סמכות מעשה שתוצאותיו יהיו מניעת שירותי מחשב או שיבושם, בכוונה להביא לתוצאות אלה, דינו - מאסר שבע שנים.

(ב) הוראות סעיף קטן (א) לא יחולו על הימנעות עובד מעבודה עקב שביתה אגב סכסוך עבודה.

4. גרימת תוצאות משובשות

(א) העורך תוכנה, מעבירה לאחר, או מפעיל מחשב בתוכנה, ביודעו שהיא תביא לתוצאות משובשות לגבי מטרת השימוש בה, והיה לו יסוד סביר להניח שאדם אחר ישתמש בתוכנה בהפעלת מחשב או יסתמך על פלט מחשב שהופעל על פיה, דינו - מאסר שבע שנים.

(ב) המספק נתונים, מעבירם לאחר, או מפעיל מחשב בנתונים או במידע, ביודעו שהם יביאו לתוצאות משובשות לגבי מטרת השימוש בהם, והיה לו יסוד סביר להניח שאדם אחר ישתמש בנתונים או במידע בהפעלת מחשב או יסתמך על פלט מחשב שהופעל על פיהם, דינו - מאסר שבע שנים.

5. **שימוש במחשב או בתוכנה להשיג דבר שלא כדין**
המשתמש במחשב או בתוכנה או גורם לשימוש בהם, בכוונה להשיג דבר שלא כדין, לעצמו או לאחר, או בכוונה למנוע דבר שלא כדין מן הזולת, דינו - מאסר חמש שנים.

6. **פגיעה בתוכנה, נתונים, או מידע בכוונה להשיג דבר**
המוסיף על תוכנה, על נתונים או על מידע המשמשים או עשויים לשמש מחשב, או גורע מהם, ללא סמכות, בכוונה להשיג דבר לעצמו או לאחר, או בכוונה למנוע דבר מן הזולת, דינו או - מאסר חמש שנים.

7. **מניעת חפץ המגלם תוכנה בכוונה להשיג דבר**
המונע שלא כדין מבעליו או מהמחזיק בו כדין, חפץ המגלם תוכנה, נתונים או מידע המשמשים או עשויים לשמש מחשב, בכוונה להשיג דבר לעצמו או לאחר, או למנוע דבר מן הזולת, דינו - מאסר חמש שנים.

8. **השגת תוכנה שלא כדין**
המשיג, לעצמו או לאחר, תוכנה שלא כדין, דינו - מאסר חמש שנים.

9. **הסתמכות על פלט כוזב**
המסתמך על פלט-מחשב במצג לזולתו בקשר לעיסקה או לחוות דעת מקצועית, כשהוא יודע שהפלט כוזב, דינו - מאסר חמש שנים.

10. **תחולה**
הוראות פרק זה לא יחולו אלא כשהמחשב, התוכנה, הנתונים או המידע, לפי הענין, משמשים או מיועדים לשמש אחד מאלה -
(1) המדינה או תאגידים המספקים שירות לציבור;
(2) עסק, תעשיה, חקלאות, שירותי בריאות או מטרות מדע.

11. **הגנה**
תהא זו הגנה טובה לנאשם על פי סעיף 4 אם יוכיח שגילה את הפגם לאדם האחר, או שאיפשר את הגילוי, לפני השימוש בתכנה, בנתונים או במידע.

12. **הימנעות**
בית המשפט רשאי שלא להרשיע אדם בעבירה על סעיף 2, 3 או 4, אף אם הוכחה אשמתו, אם ראה שהפגיעה אינה חמורה והעבירה לא נעברה בזדון; אין באי הרשעה כאמור כדי למנוע הרשעת הנאשם בעבירה אחרת שהוכחה בשל אותו מעשה.

13. **סייג לתפיסה**
על אף האמור בכל דין אחר, לא ייתפס, בחקירה בעבירה, מחשב או חלק ממנו, לרבות אמצעי האוגר נתונים, מידע או תוכנה, אלא על פי צו של בית המשפט; צו כאמור שניתן שלא במעמד הבעלים או המחזיק יהא תקף למשך 24 שעות בלבד, ולא יוארך אלא לאחר שניתנה לבעלים או למחזיק הזדמנות להשמיע דברים; לענין זה לא יבואו שבתות ומועדים במנין השעות.

14. **הודעה על עבירה**
(א) היה לממונה בשירות המדינה, וכן בתאגידים המספקים שירות לציבור והעוסקים בסוגי עיסוקים שייקבעו בתקנות, יסוד סביר לחשוד כי אדם שהוא ממונה עליו עבר עבירה לפי סעיפים 2 עד 8, במחשב שבאותו מוסד או עסק בו עסק עובד הממונה, יודיע על כך בהקדם האפשרי למשטרה; העובר על הוראה זו, דינו - מאסר שנה.
(ב) ממונה יהיה פטור מהחובה האמורה בס"ק (א) אם היה לו, באותו מוסד או עסק, ממונה - שעליו, והיה לו יסוד סביר להניח שדבר החשד וסיבותיו היו ידועים לממונה-שעליו.
(ג) לענין סעיף זה, "ממונה" - מעביד או מי שממונה על עובד מטעמו של המעביד, ושוכרו של קבלן לגבי הקבלן או עובדו.

סימן ב': חדירה למחשב למטרות מיוחדות

15. **הגדרות**
בסימן זה -
"חדירה למחשב" - השגת תוכנה, נתונים ומידע האצורים בו, והשגת פלט-מחשב ממחשב.
"שר" - ראש הממשלה או שר הבטחון.

"רשות בטחון" - כל אחד מאלה;
(1) אגף המודיעין במטה הכללי של צבא-הגנה-לישראל;
(2) שירות הבטחון הכללי.
"קצין משטרה מוסמך" - קצין משטרה בדרגת ניצב-משנה ומעלה, שהסמיך המפקח הכללי של המשטרה.

16. **חדירה למחשב מטעמי בטחון**
(א) שר רשאי, אם נתבקש לכך על ידי ראש רשות בטחון, ואם שוכנע כי הדבר דרוש מטעמי בטחון המדינה, להתיר בכתב חדירה למחשב.
(ב) בהיתר לפי סעיף זה יתוארו זהות המחזיק במחשב, ומקומו של המחשב, במידה שהם ידועים, ודרכי החדירה.
(ג) בהיתר תפורש תקופת תקפו; התקופה לא תעלה על שלושה חדשים מיום נתינת ההיתר; ההיתר ניתן לחידוש מדי פעם לפעם.
(ד) היה ההיתר מאת שר הבטחון - יודיע שר הבטחון מיד לראש הממשלה על מתן ההיתר או על חידושו; שר יודיע לשר המשפטים אחת לשלושה חודשים על היתרים שנתן לפי סעיף זה.

17. **חדירה למחשב למניעת עבירות**
(א) נשיא בית משפט מחוזי, ובהעדרו - נישא תורן של בית משפט מחוזי, רשאי, לפי בקשת קצין משטרה מוסמך, להתיר בצו חדירה למחשב, אם שוכנע שהדבר דרוש למניעת עבירות או גללוי עבריינים.
(ב) הבקשה תידון במעמד צו אחד בלבד, ומטעם המבקש יתייצב קצין בדרגת סגן-ניצב ומעלה.
(ג) סירב השופט להעניק היתר כמבוקש, רשאי היועץ המשפטי לממשלה או נציגו לערער על ההחלטה לפני שופט של בית המשפט העליון שנשיאו מינה לכך.
(ד) בהיתר לפי סעיף זה יתוארו זהות המחזיק במחשב ומקומו של המחשב, במידה שהם ידועים, ודרכי החדירה.
(ה) בהיתר תפורש תקופת תקפו; התקופה לא תעלה על שלושה חדשים מיום נתינת ההיתר; ההיתר ניתן לחידוש מפעם לפעם.
(ו) המפקח הכללי של המשטרה יגיש מדי חודש דין וחשבון לשר המשטרה על ההיתרים שניתנו לפי סעיף זה ועל תנאיהם; שר המשטרה יעביר העתקים מדו"חות אלה לשר המשפטים אחת לשלושה חודשים.

18. **שמירת מידע וביעורו**
שר המשפטים, באישור ועדת החוקה חוק ומשפט של הכנסת, יתקין תקנות לענין שמירת המידע שהושג בהיתר על פי סימן זה, ולענין ביעורו.

פרק ג': נזיקין

19. **עוולות**
דין מעשה או מחדל האמורים בסעיפים 2-9 כדין עוולה לפי פקודת הנזיקין (נוסח חדש).

20. **פירושים**
תוכנה, מידע ונתונים יהיו "נכס" לענין פקודת הנזיקין (נוסח חדש) ולענין סעיף 19, ורואים שינויים, העתקתם ושימוש בהם בגדר "נזק".

21. **תחולה**
הוראות פרק זה יחולו בין שהמחשב, התכנה, הנתונים או המידע הם מן האמורים בסעיף 10 ובין שאינם כן.

22. **שמירת זכויות**
אין בהוראות פרק זה כדי לגרוע מזכות תביעה לפי כלדין.

פרק ד': זכויות מחברי תוכנה

גירסה א'

23. הגדרה

"תוכנה חדשה" לענין חוק זה - תוכנה שהיא פרי מאמציו הרוחניים של מחברה.

24. זכויות מחבר התוכנה

למחבר תוכנה חדשה ולחליפו (בפרק זה - מחבר) תהיה הזכות שהמעשים המפורטים להלן לא ייעשו בתוכנה, לרבות בחלק ממנה, שלא בהסכמתו -

(1) אחסון התוכנה, או שימוש בה, במחשב;

(2) שימוש בתוכנה לשם הכנת תוכנה מקבילה או תוכנה שבעיקרה דומה לה;

(3) העתקת התוכנה בדרך אלקטרונית, אלקטרומגנטית או בכל דרך אחרת;

(4) גילוי התוכנה או חלק ממנה שהוא מקורי לפני שניתנה גישה אליה לציבור על ידי המחבר;

(5) החזקת חפץ שבו התוכנה מגולמת למטרת מכירה או עיסקה אחרת בה; לענין הוראה זו - חזקה על החזקת תוכנה חדשה שהיא נעשית למטרה כאמור, אולם בית המשפט רשאי, בנסיבות שימצא לנכון, לחייב את התובע להוכיח מטרה זו;

(6) לעשות בה עיסקה, לייבאה או לייצאה.

25. דין מחבר תוכנה דומה

הזכויות לפי סעיף 24 יהיו גם למי שחיבר באופן עצמאיתוכנה חדשה זהה או מקבילה, או שבעיקרה היא דומה לתוכנית המחבר, וההגבלות לפי אותו סעיף לא יחולו נגדו, נגד חליפו, וכן נגד מי שרכש זכויות בתוכנה מן המחבר האחר.

26. פקיעת הזכויות

הזכויות לפי סעיף 24 יפקעו בתום חמש עשרה שנים ממועד חיבור התוכנה, אולם הן תפקענה בתום עשר שנים אם לא ארע תוך עשר שנים אחד מאלה:

(1) השתמשו בתוכנה שימוש מסחרי בישראל או מחוצה לה, בהסכמתו של המחבר, לתפעול מחשב;

(2) התוכנה הוצעה למכירה לציבור, בהסכמת המחבר.

27. סעדים

(א) הופרה זכותו של מחבר לפי חוק זה, יהיה בית המשפט מוסמך לפסוק לו פיצויים בשל ההפרה, זולת כנגד מי שרכש את התוכנה בתום-לב בשוק הפתוח.

(ב) הופרה זכותו של מחבר לפי חוק זה, או היה לבית המשפט חשש שעומדים להפירה, יהיה בית המשפט מוסמך, לבקשת המחבר, ליתן צו-מניעה לשם מניעת ההפרה.

(ג) הגיעה לידי אדם שלא כדין תוכנה שיש עליה זכות מחבר לפי חוק זה, רשאי בית המשפט, לבקשתו של המחבר, לצוות על מסירתה, או מסירת החפץ שבו היא מגולמת, לידי המחבר.

28. הודעה על זכויות

(א) לא תועבר תוכנה שיש עליה זכות לפי פרק זה, על ידי המחבר או על ידי אדם אחר, לזולתו, אלא בצירוף הודעה בכתב על קיומה של זכות כזאת, שם בעל הזכות ומועד פקיעתה, ככל הידוע למעביר.

(ב) הועברה תוכנה ללא הודעה כאמור, יהיה המעביר אחראי לכל הפרה שיכול היה לצפותה בזמן ההעברה.

29. שמירת זכויות

הוראות פרק זה באות להוסיף על כל דין המקנה זכות למחבר תוכנה ולא לגרוע ממנו.

30 תחולה על תוכנה שחוברה מחוץ לישראל

חוק זה לא יחול לגבי תוכנה שחוברה מחוץ לישראל אלא במידה ששר המשפטים קבע תחולתו לגביה, ויכול שר המשפטים לקבוע כאמור לפי מקום החיבור או בכל דרך אחרת.

גירסה ב' (אם תתקבל גירסה זו, ישונה המיספור של שאר הסעיפים)

23. זכויות מחברי תוכנה
יראו "תוכנה" לכל דבר וענין, כיצירה ספרותית כמשמעות בחוק זכות יוצרים, 1911.

פרק ה': ראיות

31. אמינות פלט מחשב וקבילותו
(א) חזקה לכאורה היא לגבי פלט מחשב -
(1) כשהפלט הוא תוצאה של הזנה - כי נתוני ההזנה שבו הם כפי שנרשמו במקור שממנו הוזן המחשב, אם הוכחו אמינות ההזנה, הקליטה והפליטה של המחשב;
(2) כשהפלט הוא תוצאה של הזנה עצמית - כי נתוני ההזנה העצמית שבו הם כפי שנקלטו על ידי המחשב, אם הוכחו אמינות הקליטה והפליטה של המחשב.
(3) כשהפלט הוא תוצאה של עיבוד נתונים או הערכה - כי עיבוד הנתונים וההערכה של המחשב הם אמינים, אם הוכחו אמינות ההפעלה ופעולת החומרה, ותקינות התוכנית שלפיה עובדו הנתונים או נתקבלה ההערכה.
(ב) נבע הפלט משיתוף במערכות מחשבים, יחולו הוראות סעיף קטן (א) לגבי כל מחשב שבמערכת, לפי הענין.

32. רישום על ידי גוף ציבורי או במהלך עסקים
(א) שימש מחשב לרישום, לעיבוד נתונים או להערכה, על על ידי גוף ציבורי במילוי תפקידו, או במהלך הרגיל של מסחר או עסק אחר כשאותו שימוש הוא חלק מהמהלך הרגיל כאמור, עומד הפלט של אותו מחשב על חזקתו כאמור בסעיף 31(א) אף ללא או הוכחת הפרטים האמורים לפי הענין.
(ב) נתקיימו במחשב התנאים האמורים בס"ק (א) והיה זה המהלך הרגיל של אותו גוף או עסק להסתמך על אמיתות רישומים מסוג זה, יהא הרישום קביל גם כראיה לכאורה לאמיתות תכנו.

33. דרכי הוכחה מאושרים
שר המשפטים רשאי לקבוע בתקנות את האופן והתנאים להוכחת אמינות או תקינות לענין סעיף 31; קבע אופן או תנאים כאמור, לא תוכח אמינות או תקינות אלא באופן שנקבע, זולת אם התיר בית המשפט הוכחה בדרך אחרת.

34. שמירת דינים
אין באמור בפרק זה כדי לגרוע מטענה בדבר קבילותו של פלט מחשב כראיה זולת היותו ראיה שאינה ישירה ושאינה מפי עד.

פרק ו': הוראות שונות

35. תיקון חוק הגבלים עסקיים
בסעיף 6 לחוק ההגבלים העסקיים, התשי"ט-1959, במקום "או בזכות יוצרים" יבוא "בזכות יוצרים בזכות לפי הפרק השלישי לחוק המחשבים (עבירות, הגנת תוכנה וראיות) התשמ"ז-1987.

36. הוראות מעבר
(א) הוראות פרק ב' לא יחולו לגבי מעשים שנעשו לפני תחילתו של חוק זה.
(ב) הוראות פרק ג' יחולו על תוכנה שחוברה לפני תחילתו של חוק זה, אך לא יחולו על הפרה שנעשתה לפני תחילתו של חוק זה.
(ג) הוראות סעיף 28 לא יחולו על תוכנה שחוברה לפני תחילתו של חוק זה.

37. ביצוע ותקנות
שר המשפטים ממונה על ביצוע חוק זה והוא רשאי להתקין תקנות בכל הנוגע לביצועו.

נספח ב

ניהול אבטחת מידע במחשבים אישיים

מאיר פלג
באדיבות מערכת "קווים המשרד"

מבוא ורקע

הדיון שלהלן מותאם הן למחשבים אישיים המתפקדים כתחנות עצמאיות והן למחשבים אישיים הפועלים כתחנות ברשת. מוצגים כאן העקרונות הכלליים של האבטחה במחשבים אישיים ואין התייחסות לטכנולוגיה מסוימת אשר עשויה להשתנות.

בבחינת אבטחת מידע במחשבים אישיים מתמצה הצורך להגן על מידע האגור הן בארגונים גדולים שבהם עיבודי המידע מבוזרים והן בארגונים קטנים וקטנים מאוד המעבדים מידע באמצעות מחשב אישי. קבצי תכתובת במעבד תמלילים אינם מיועדים לעיון של כל אחד, וכך גם קבצי נתונים רפואיים אצל רופא, אשר משתמש במחשב אישי לניהול המרפאה. בשני המקרים אין רוצים שגורמים נוספים יחזו במידע.

רוב יצרני המחשבים האישיים אינם עוסקים בסוגיית האבטחה. הפתרונות השגרתיים של בתי תוכנה כוללים נעילה פיסית כל כונני הדיסק הקשיח, או התקליטון והצפנה של קבצי המידע. אפשר גם לרכוש כרטיס חומרה (מתאים לסוג מחשבים מסוים בלבד), אשר אינו מאפשר להתחל את מערכת ההפעלה, אלא אם תוקש על ידי המשתמש סיסמה מוגדרת. ניתן להכניס שיפורים נוספים בכרטיס החומרה, אך הדבר מותנה כמובן בתקציב, במידת הסודיות הנדרשת ובנכונות להשקיע כדי להגן על המידע.

בהסתמך על ניסיונו של המחבר, יש לפעול ולטפל בשלוש גישות:

1. להעריך את חשיבות המידע אשר מטופל במחשב האישי.
2. להעריך את הסיכונים כתוצאה מחשיפת או הרס מידע זה.
3. להעריך מה הן הדרכים הנאותות להפחתת הסיכונים למידה סבירה ומתקבלת על הדעת.

צעדים ראשונים

חובה ליצור מדיניות כלל ארגונית ואסטרטגיה לפיקוח ובקרה של תפעול מחשבים אישיים. מדיניות זו יכולה להיות חלק ממדיניות ענ"א הכוללת בחברה או להיות יחודית לגבי המחשבים האישיים. המדיניות חייבת להיות גמישה דיה, אך עם זאת ניתנת לאכיפה על כל יחידות הארגון. במקביל יש לאתר את גורמי ההנהלה המעוניינים ולהבטיח את תמיכתם במדיניות האמורה.

בדרך כלל ימונה גורם מרכזי אחד בודד שיהיה אחראי למחשבים אישיים בארגון, הן מבחינת החומרה והן מבחינת התוכנה. גורם ריכוזי זה יקל על השליטה בנושא ועל אכיפת המדיניות שתותלט. בניהול נכון תקטן ההוצאה העתידית וההשקעה במחשבים, בציוד נלווה, בציוד גיבוי, תקליטונים, נייר וכו'. בניהול נכון יקטן מספר הקריאות לשירות, ניתן יהיה להגיע להסכמי כמויות עם יבואני הציוד ועוד.

גורם מרכזי זה חייב להיות במסגרת יחידה ארגונית המטפלת במערכות מידע ואו"ש בארגון ובעמדת ניהול בכירה. האחראי לנושא חייב להיות בעל רקע עשיר הן במחשבים גדולים והן במחשבים אישיים ומנוסה בהקמת מערכות מידע אישיות. רצוי שיהיה מנוסה בהוראה והדרכה בנושאי מחשב.

הגדרות ויעדים

צריך להגדיר את משאבי המידע האגורים במחשבים אישיים ולציין את אלה שיש להגן עליהם במיוחד. רצוי אף לדרג אותם על פי סדר העדיפות בהגנה על המידע. אם יש מידע מסווג, יש להגדיר את כל פריטי המידע אשר לא רצוי שינוהלו במחשבים אישיים, אלא במערכת מחשב מרכזית מאובטחת. במקביל יובהר למשתמשים במחשבים אישיים, כי הם ורק הם אחראים באופן ישיר ואישי הן לציוד והן למידע האגור בו. יודגש בפניהם כי לעתים ערך המידע עולה על ערך המחשב.

במסגרת ההדרכה השוטפת למשתמשים, יש להקדיש פרק הדן באבטחת המידע והציוד. הדרכה זו תינתן בדרך כלל לפני רכישת הציוד או לפני חיבור לרשת תקשורת מחשבים בארגון. רצוי לתכנן פרק לימוד בנושא אבטחת שכל משתמש יהיה חייב בו פעם בשנה. כדאי שסיסמת אבטחה תקופתית, או אקראית, תופיע עם טעינת מערכת ההפעלה DOS לאחר הדלקת המחשב.

המחשב האישי איננו רכוש פרטי של העובד, ולכן זכותו של המעביד לערוך ביקורת ולראות תדפיס של הקבצים המאוחסנים על גבי הדיסק או התקליטונים. חובה לעגן בנוהל כתוב את הרשאות השימוש במחשבים האישיים, הן מבחינת המורשים להשתמש והן מבחינת העבודות המותרות לביצוע. בנוהל יוגדר מה יהיו האמצעים שינקטו כלפי משתמש לא מורשה, או משתמש מורשה שייתפס בביצוע מעשים שלא הותרו. בנהלים מבהירים למשתמשים כי גישה למחשב איננה מקנה להם כל זכות גישה לקבצים לא להם. כאמור, ההנהלה חייבת לקבוע מתאם פעילויות בתחום המחשבים האישיים, אשר יהא אחראי להתווית מדיניות הפעלה ומדיניות אבטחת מידע.

אבטחת מידע בתקשורת
בין מחשבים אישיים לבין מחשבים מרכזיים

למחשבים ניידים, במיוחד לאלה אשר קשורים בחיוג למחשב המרכזי, יש להגדיר נהלי שימוש ונהלים לאבטחת מספר החיוג מפני שימוש בלתי מורשה. אסור לשמור ליד המחשב מדבקה או מסמך כלשהו הנושא מספרי חיוג, סיסמאות, קודים וכו'.

על מנת להגן על המידע במחשב המרכזי יש להשתמש בתוכנות אבטחת מידע ו/או בשיטת הקריאה החוזרת (call back), בה המחשב המרכזי "מחזיר חיוג" אל המחשב האישי המתקשר, לאחר שזיהה את המשתמש בו. אפשר לדרוש באופן אקראי מן המשתמש במחשב האישי להזדהות שוב במהלך עבודתו באמצעות סיסמת הכניסה למערכת, או סיסמה מוסכמת אחרת. אם שוגים בהקשת סיסמה, יש להגביל את מספר ניסיונות ההקשה שלה, כדי להגן מפני חדירה בשיטת "ניסיון וטעיה" (trial and error) הנהוגה בתקשורת שבין מחשבים אישיים לבין מחשב מרכזי. יש למנוע, בסיוע תוכנה, את ההקרנה ו/או הדפסה של מלות המפתח המוקשות בזמן ההתקשרות למערכת.

משתמש נבון ייצור טבלה שבאמצעותה ייבדק מקור הקשר של מציגי הסיסמאות. כלומר, למקור קשר מסוים ומוגדר מותר יהיה לפתוח בהתקשרות רק כאשר הוא משתמש בסיסמאות מסוימות. דבר זה יסייע במידת מה למניעת התקשרות זרה לערוץ תקשורת מורשה. תוקם מערכת בקרות ודיווחים לאיתור מידע לגבי קבצים בשימוש שוטף ובמיוחד לגבי העברת קבצים מהמחשב המרכזי למחשב האישי ולהיפך.

שליטה ובקרה

האחראי לאבטחה יקבע נוהלי טיפול באמצעים לאחסון מידע: הגנה מפני חום, לכלוך, מים ופגעי אדם וטבע אחרים. יש לקבוע בנוהל כי אין להותיר בכוננים תקליטונים, או קלטות. רצוי שתקליטון לא יימצא בכונן בזמן הדלקה או כיבוי של המחשב. רצוי להמנע מעירוב של תכניות וקבצי נתונים באותו אמצעי אחסון.

חובה להתייחס לאמצעי אחסון מגנטיים מבחינת אבטחתם כאל כל אמצעי קריא אחר. יש לשמור בכספת חסינת אש אמצעי אחסון הנושאים מידע רגיש. רצוי לקבוע נוהלים לזיהוי חד משמעי של קבצי המידע ואמצעי האחסון השונים: הן המקור והן הגיבוי (שם, תאריך ייצור, תאריכי שימוש, שם יוצר המידע וכו').

אמצעי אחסון מגנטיים פגומים יש להשמיד ע"י הרס כדי שלא ניתן יהיה לאתר ולזהות המידע האגור בהם באמצעות מיכשור. צריך לקבוע הנחיות להשמדה או מחיקה של מידע בתקליטונים ו/או בדיסקים. בדרך כלל ניתן להסתפק בתוכנית שירות הכותבת בהם מספר פעמים נתונים אקראיים. כאשר המידע באמצעי האחסון הוא מסווג ורגיש מומלץ להשתמש גם בציוד מחיקה אלקטרו-מגנטי.

אמצעי בקרה בתוכנה ותיעוד

חובת ההנהלה להבהיר לציבור המשתמשים מה הם זכויות על מידע, בעלות על מידע, זכויות יוצרים וחוקי מדינה המטפלים בסוגיות מידע וצנעת הפרט. האחראי לכך יצור מערכת תיעוד מסודרת ועקבית לכל טיפול בתוכנה או בפריטי מידע.

גורם מרכזי יבחן את התוכנות היישומיות במחשבים האישיים בארגון. עבודה זו מכוונת למנוע כפילויות בכתיבת תוכנות, לחסוך במשאבים ולאפשר לאתר תקלות צפויות בשל אי התאמות בממשקי תוכנה שונים.

מבקר פנימי ידאג לטפל בביקורת ענ"א במערכות אישיות ויראה זאת כמשימת קבע. המבקר יבדוק תוצאות של עיבודים במחשבים אישיים מול תוצאות חזויות, על מנת לאפשר איתור של ליקויים בביצוע, או שיבושים אחרים מכוונים, או בשוגג.

אבטחה פיסית

מערכת נהלים צריכה לתמוך במעקב אחר מיקום של כל מחשב אישי, אמצעי האבטחה של הנתונים שבו ואמצעי הבטיחות סביבו. צריך לסמן את חלקי המחשב השונים בזיהוי הבעלים ומספור סידורי חד ערכי שאיננו ניתן להסרה, מחיקה או טשטוש בנקל.

רצוי להתקין מיכשור להגנה מפני מפל מתח העלול לפגוע בנתונים ולהזיק למחשב. אם מופעלים יישומים קריטיים, צריך להבטיח מקור אנרגיה חליפי לרשת החשמל. במקום שיש בו חשש מחדירת מים, צריך לכסות את המחשב בכיסוי עמיד במים בגמר השימוש בו. חשוב לתחזק כראוי את ציוד כיבוי האש ואת מטפי גז הלון המיועדים לכיבוי שריפה בציוד מחשב.

אין להתקין מחשבים אישיים באיזורים בלתי מאויישים, או שיש בהם תנועת בני אדם שאינם עובדי הארגון (שטחים ציבוריים). אין להתקין מחשבים בקומות תחתונות ליד חלונות שאינם מסורגים. המידע הוא נכס ועל כן יש צורך להתקין אמצעי מיגון, כמו סורגים, מערכות אזעקה וגלאים (אש, עשן ולחות). אפשר לקבע את המחשב בשולחן שעליו הוא מוצב, למניעת גניבה אפשרית. אפשר להתקין מנעול כדי למנוע את הפתיחה של תיבת המחשב לשם גניבת כרטיסים או הוצאת הדיסק הקשיח ממקומו. ניתן גם לשלב אזעקה בתוך ארגז המחשב, אשר תופעל כאשר ייעשה ניסיון בלתי מורשה לפתוח את המכשיר או לסלקו ממקומו. כדאי להוסיף מפתח ו/או כרטיס זיהוי מגנטי שבלעדיהם לא ניתן יהיה להפעיל את המחשב.

סיכום

בפרק זה ניסיתי להקיף את נושאי ההבטחה מבלי להכנס לפירוט מעמיק בכל אחד מתחומי האבטחה של מחשבים אישיים. עם זאת, בטוחני שהקורא יוכל להסתייע בדברים אלה כדי ללמוד כיצד ניתן להגן על המשאבים והמידע ברמת ההגנה הממוצעת הנדרשת. תחום עיסוק חדש ומתפתח זה קרוי "אבטחת מידע".

ביבליוגרפיה

הרשימה הביבליוגרפית כוללת מספר חלקים:

א. פרסומים שונים שיצאו לאור בעברית,
ב. הרשימה המקורית אשר המחבר מתייחס אליה בספר,
ג. ספרים ופרסומים באנגלית שיצאו לאור לאחרונה.

פרסומים בעברית

-/הנחיות לנוהלי מבדק וביקורת במערכות מידע ממוכנות / המועצה העליונה להכוונת ענ"א להליכי מינהל, 1975.
-/מחשבים: פשעים, רמזים ובקרות, מדריך למנהל / המכון לפריון העבודה והייצור, 1987.
בר-חוה נורי / הנחיות לנוהלי בקרה וביקורת במערכות מידע ממוחשבות / המכון לפריון העבודה והייצור, 1985.
כהני מנחם / נוהל מסגרת לגיבוי מתקני מחשב / המכון לפריון העבודה והייצור, 1987.
נורי בר-חוה וד"ר משה תלם / מחשבים וסיכונים / צ'ריקובר, 1983.
עילם פיליפ ג. / רשימת תיוג להערכת סדרי האבטחה בענ"א / המכון לפריון העבודה והייצור, 1985.

מאמרים שונים פורסמו בתקופונים, בעתונות המקצועית ובעתונות הכללית.

- אנשים ומחשבים.
- במענ"א / בטאון של מבקרי ענ"א.
- מחשבים / מירב תעשיות הפקה.
- מידעון / איגוד מנתחי מערכות לענ"א.
- מעשה חושב / איל"א.
- קווים המשרד / זווית אחרת.
- רשת מחשבים / מירב תעשיות הפקה.

- מאמרים בנושא אבטחה מתפרסמים ע"י איגוד מנתחי מערכות לענ"א ועל ידי איל"א במסגרת הכנסים השנתיים של ארגונים אלה.

הרשימה הביבליוגרפית המקורית

Achugbue, J.D. and Chin, F.Y. (1979). The effectiveness of output modification by rounding for protection of statistical databases. *INFOR*, Vol. 17, No. 3, 209–18

Adleman, N. (1976). *Engineering Investigations in Support of Multics Security Kernal Software Development*, ESD-TR-77-17, Honeywell Information Systems Brighton, Mass.

AFIPS (1974). *System Review Manual on Security*, American Federation of Information Processing Societies, Arlington, Virginia

AFIPS (1979). *Security – Checklist for Computer Center Self Audits*, American Federation of Information Processing Societies, Arlington, Virginia

Anderson, J.P. (1972). Information security in a multi-user computer environment. In *Advances in Computers, Vol. 12* (ed. M. Rubinoff), Academic Press, New York

Apple (1982). *Copy II Plus – an Apple Disk Utility System*, Apple Computer, Inc., Portland, Oregon, chapter 4 (entitled Diskette Protection Schemes)

Ashby, R.W. (1976). *An Introduction to Cybernetics*, Methuen, London

Attanasio, C.R., Markstein, P.W. and Phillips, R.J. (1976). Penetrating our operating system – a study of VM370 integrity. *IBM Systems Journal*, Vol. 15, No. 1, 102–16

Audit Commission (1985). *Computer Fraud Survey*, HMSO, London

Baran, P. (1964). *On Distributed Communications – Security and Secrecy*, RM-3765-PR, RAND Corporation, Santa Monica, California

BBC (1981). *Transcript of Panorama Programme of 2nd March 1981*, British Broadcasting Corporation, London

Beck, L.L. (1979). *A Security Mechanism for a Statistical Database*, Department of Computer Science, Southern Methodist University, Dallas, Texas

Black, G. and Karten, H. (1983). US scuttles the pirates. *Computer Weekly*, No. 876, 1

British Computer Society (1981). *Control and Audit of Minicomputer Systems*, Heyden, London

Broadbent, D. (1979). *Contingency Planning*, NCC, Manchester

Bunyan, A. (1979). Police and national security. In *Computers, Records and the Right to Privacy* (ed. P. Hewitt), Input Two-Nine, Purley

Checkland, P. (1981). *Systems Thinking, Systems Practice*, Wiley, Chichester

Chin, F.Y. and Ozsoyoglu, G. (1980). Security of statistical bases. In *Advances in Computer Security Management, Vol. 1* (ed. T.A. Rullo), Heyden, London, 57–8

Cmnd 4407 (1970). *British Patent System* (Chairman, M.A.L. Banks), HMSO, London

Cmnd 5012 (1972). *Report of the Committee on Privacy* (Chairman, The Rt Hon K. Younger), HMSO, London

Cmnd 6353 (1975). *Computers and Privacy*, HMSO, London
Cmnd 6732 (1977). *Copyright and Design Law*, HMSO, London
Cmnd 7341 (1978). *Report of the Committee on Data Protection* (Chairman, Sir N. Lindop), HMSO, London.
Cmnd 8302 (1981). *The Reform of the Law Relating to Copyright*, HMSO, London
Conway, R.W., Maxwell, W.L. and Morgan, H.L. (1972). On the implementation of security measures in information systems. *Communications of ACM*, Vol. 15, No. 4, 211–20
Cornish, W.R. (1981). *Intellectual Property: Patents, Copyright, Trade Marks and Allied Rights*, Sweet and Maxwell, London
Court, J.M. (1984). *Personal Data Protection – The 1984 Act and its implications*, NCC, Manchester
Courtney, R.H. (1977). Security risk assessment in electronic data processing systems. *AFIPS Conference Proceedings, NCC*, Vol. 46, 97–104
Datapro (1985). *Computer Weekly/Datapro Survey – British User Ratings of Computer Systems*, Datapro, CH-1164, Burchillon, Switzerland
Davis, K.W. and Perry. W.E. (1982). *Auditing Computer Applications*, Wiley, New York
Deloitte, Haskins and Sells (1982). *The External Auditor as Privacy Inspector*, NCC, Manchester
Denning, D.E.R. (1982). *Cryptography and Data Security*, Addison-Wesley, Reading, Massachusetts
Denning, D.E.R. and Denning, P.J. (1977). Certification of programs for secure information flow. *Communications of ACM*, Vol. 20, No. 7, 504–13
Denning, D.E.R. and Denning, P.J. (1979). Data security. *ACM Computing Surveys*, Vol. 11, No. 3, 227–49
Diffie, W. and Hellman, M.E. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, Vol. 11, No. 22, 644–54
Diffie, W. and Hellman, M.E. (1977). Exhaustive cryptanalysis of the NBS data encryption standard. *Computer*, Vol. 10, No. 6, 74–84
Dobkin, D., Jones, A.K. and Lipton, R.J. (1976). *Secure Databases: Protection against User Inference*, Research Report 65, Department of Computer Science, Yale University, New Haven, Connecticut
Enticknap, N. (1982). Patent granted after ten year legal tussle. *Computer Weekly*, 29 July, 6
Farquhar, W. and Wong, K.K. (1983). *Computer Crime Casebook*, BIS Applied Systems, London
Fenton, J.S. (1974). Memoryless subsystems. *Computer Journal*, Vol. 17, No. 2, 143–7
Fernandez, E.B., Summers, R.C. and Wood, C. (1981). *Database Security and Integrity*, Addison-Wesley, Reading, Massachusetts
FIPS 31 (1974). *Guidelines for Automatic Data Processing, Physical Security and Risk Management*, FIPS PUB 31, National Bureau of Standards, Washington, DC
FIPS 46 (1977). *Data Encryption Standard*, FIPS PUB 46, National Bureau of Standards, Washington, DC
FIPS 65 (1979). *Guidelines for Automated Data Processing Risk Analysis*, FIPS PUB 65, National Bureau of Standards, Washington, DC
FIPS 73 (1980). *Guidelines for Security of Computer Applications*, FIPS PUB 73, National Bureau of Standards, Washington, DC
Franz, C.R., Wilkins, S.J. and Bower, J.C. (1981). A critical review of proprietary software protection. *Information and Management*, Vol. 4, 55–69

Friedman, S. (1982). Contingency and disaster planning. *Computers and Security*, Vol. 1, No. 1, 34–40

Gaines, R.S. and Shapiro, N.Z. (1978). Some security principles and their application to computer security. *Operating Systems Review*, Vol. 12, No. 3, 19–28

Gilhooley, I.A. (1980). Data security. In *Advances in Computer Security Management, Vol. 1* (ed. T.A. Rullo), Heyden, London, 33–56

Glaseman, S., Turn, R., and Gaines, R.S. (1977). Problem areas in computer security assessment. *AFIPS Conference Proceedings, NCC*, Vol. 46, 105–12

Goldstein, R.C. (1975). The costs of privacy. *Datamation*, Vol. 21, No. 10, 65–9

Gostin, L. (1984). *The Data Protection Bill – an NCCL briefing*, National Council for Civil Liberties, London

Graham R.L. (1984). The legal protection of computer software. *Communications of ACM*, Vol. 27, No. 5, 422–6

Grover, D.J. and Hart, R.J. (1982). Computing and reform of copyright protection. *Computer Bulletin*, Vol. II, No. 31, 4–5

Harrison, M.A., Ruzzo, W.L. and Ullman, J.D. (1976). Protection in operating systems. *Communications of ACM*, Vol. 19, No. 8, 461–71

Hartson, R. and Hsaio, D.K. (1975). *Languages for Specifying Protection Requirements in Database Systems (Part 1)*, Report OSU-CISRC-TR-74-10, Ohio State University, Computer and Information Science Research Center, Columbus, Ohio

Hayhurst, W. (1982). Pythagoras and the computer. *EIPR*, Vol. 8, 223–7

Highland, H.J. (1983). Impact of microcomputers on total computer security. *Proceedings of IFIP Security Conference*, North-Holland, Amsterdam, 119–29

Hoffman, L.J. (1977). *Modern Methods for Computer Security and Privacy*, Prentice-Hall, Englewood Cliffs, New Jersey

Hoffman, L.J. (1980). *Computers and Privacy in the Next Decade*, Academic Press, New York

Hoffman, L.J. and Miller, W.F. (1970). Getting a personal dossier from a statistical data bank. *Datamation*, Vol. 16, No. 5, 74–5

Hoffman, L.J., Michelman, E.H. and Clements, D. (1978). Securate – security evaluation and analysis using fuzzy metrics. *AFIPS Conference Proceedings, NCC*, Vol. 47, 531–40

Hsiao, D.K., Kerr, D.S. and Madnick, S.E. (1979). *Computer Security*, Academic Press, New York

IBM (1974). *Data Security and Data Processing, Volume 3, Part 1, State of Illinois: Executive Overview*, G320-1372-0, IBM, New York

IBM (1976). *Data Security Controls and Procedures – a Philosophy for DP Installations*, G320-5649-00, IBM, New York

Kahn, D. (1967). *The Codebreakers*, Macmillan, New York

Kimmance, P.F. (1981). *Computer Fraud Survey*, Local Government Audit Inspectorate, London

Kline, C.S. and Popek, G.J. (1979). Public key versus conventional key encryption. *AFIPS Conference Proceedings, NCC*, Vol. 48, 831–8

Lampson, B.W. (1971). Protection. *Proceedings of Information Science and Systems*, 437–43

Land, F.F. (1982). Tutorial on participative design. *Computer Journal*, Vol. 25, No. 2, 283–5

Lane, V.P. and Corcoran, J.B. (1978). Systems from conception to successful implementation in the office. *Proceedings of CAD 1978 Conference*, IPC, Sutton

Lane, V.P. and Step. J. (1985). The formidable if not insurmountable organisational problems of disaster recovery planning. *IFIP Security 1985 Conference Proceedings*, North-Holland, Amsterdam

Lane, V.P. and Wright, F.G. (1979). Human resources systematically applied to ensure computer security. *Proceedings of 2nd European Conference on Informatics, held in Venice*, Springer, Berlin

Lennon, R.E. (1978). Cryptography architecture for information security. *IBM Systems Journal*, Vol. 17, No. 2, 138–51

Linden, T.A. (1975). Operating system structures to support security and reliable software. *ACM Computing Surveys*, Vol. 8, No. 4, 409–45

Linowes, D.F. (1977). *Personal Privacy in an Information Society; the Report of the Privacy Protection Study Commission*, GPO Catalog No. Y3, P93/5.1

Lobel, J. (1980). Risk analysis in the 1980s. *AFIPS Conference Proceedings, NCC*, Vol. 49, 831–6

Loeckx, J. and Sieber, K. (1984). *The Foundations of Program Verification*, Wiley, Chichester

Martin, J. (1973). *Security, Accuracy and Privacy in Computer Systems*, Prentice-Hall, Englewood Cliffs, New Jersey

Martin, J. (1976). *Systems Performance: Human Factors and Systems Failures – Engineering Reliability Techniques*, Open University, Milton Keynes, 12–20

Maude, T. and Maude, D. (1984). Hardware protection against software piracy. *Communications of ACM*, Vol. 27, No. 9, 950–9

McLening, M. (1983). The software protection racket. *Software*, Vol. 2, No. 6, 4–12

McNulty, L. (1980). The Federal Aviation Administration computer security program. In *Advances in Computer Security Management, Vol. 1* (ed. T.A. Rullo), Heyden, London 231–45

McPhee, W.S. (1974). Operating system integrity in OS/VS2. *IBM Systems Journal*, Vol. 13, No. 3, 230–52

Miller, A.R., (1971). *Assault on Privacy*, University of Michigan Press, Ann Arbor, Michigan

Mooers, C.N. (1975). Computer software and copyright. *ACM Computing Surveys*, Vol. 7, No. 1, 45–73

Norback, C.T. (1981). *The Computer Invasion – What Information They Have on You*, Von Nostrand Reinhold, New York

Norman, A.R.D. (1983). *Computer Insecurity*, Chapman and Hall, London

Page-Jones, M. (1980). *The Practical Guide to Structured Systems Design*, Yourdon Press, New York

Parker, D.B. (1981). *Computer Security Management*, Reston Publishing, Reston, Virginia

Parker, D.B. and Madden, J.D. (1978). *ADP Occupational Vulnerabilities*, SRI International, Menlo Park, California

Parker, D.B., Nycum, S.H. and Ware, W.H. (1984). Computers crime and privacy – a national dilemma: Congressional testimony from industry. *Communications of ACM*, Vol. 27, No. 4, 312–21

Perry, W.E. (1981). *Computer Control and Security*, Wiley, New York

Peterson, J. and Silberschatz, A. (1982). *Operating System Concepts*, Addison-Wesley, Reading, Massachusetts

Reed, S.K. (1977). *Automatic Data Processing Risk Assessment*, NBS IR 77-1228, National Bureau of Standards, Washington, DC

Rivest, R.L., Shamir, A. and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of ACM*, Vol. 21, No. 2, 120–6

Rodriguez, J.J. and Fisher, P.S. (1980). Security problems in a database environment. In *Advances in Computer Security Management, Vol. 1* (ed. T.A. Rullo), Heyden, London, 122–39

Ruder, B. and Madden, J.D. (1978). *An Analysis of Computer Security Safeguards for Detecting and Preventing Computer Misuse*, NBS SP 500-25, National Bureau of Standards, Washington, DC

Rule, J.B. (1974). *Private Lives and Public Surveillance*, Allen Lane, Penguin, London

Saltzer, J.H. and Schroeder, M.D. (1975). The protection of information in computer systems. *Proc. IEEE*, Vol. 63, No. 9, 1278–308

Samocuik, M. (1982). Corporate attitudes to computer misuse; a case study. *Computer Fraud and Security Bulletin*, Vol. 4, No. 7, 1–27

Scharf, J.D. (1980). Department of Defence network security considerations. In *Advances in Computer Security Management, Vol. 1* (ed. T.A. Rullo), Heyden, London, 202–30

Schlorer, J. (1975). Identification and retrieval of personal records from a statistical data bank. *Methods of Information in Medicine*, Vol. 14, No. 1, 7–13

Schlorer, J. (1979). *Disclosure from Statistical Databases: Quantitative Aspects of Trackers*, Inst. Medizinische Statistik und Dokumentation, University Glessen, West Germany

Schweitzer, J.A. (1982). *Managing Information Security: a Program for the Electronic Information Age*, Butterworth, London

Shannon, C.E. (1951). Prediction and entrophy of printed English. *Bell System Technical Journal*, 50–64

Simmons, G.J. (1979). Symmetric and asymmetric encryption. *ACM Computing Surveys*, Vol. 11, No. 4, 305–30

Simons, G.L. (1982). *Privacy in the Computer Age*, NCC, Manchester

Smith, J.E. (1980). Risk management for small computer installations. In *Advances in Computer Security Management*, Vol. 1 (Ed. T.A. Rullo), Heyden, London, 1–32

Snyder, L. (1981). Formal models of capability based protection systems. *IEEE Transactions on Computers*, Vol. C30, No. 3, 172–81

Spear, R. (1976). *Systems Performance: Human Factors and Systems Failures – the Hixon Analysis*, Open University, Milton Keynes

Squires, T. (1980). *Computer Security – the Personnel Aspect*, NCC, Manchester

Squires, T. (1981). *Security in Systems Design*, NCC, Manchester

Stern, R.H. (1978). Protection of computer programs, Parker v Flook. *EIPR*, vol. 1, 37–8

Stern, R.H. (1982). The case of the purloined object code: can it be solved? Part 1: The problems. *Byte*, September, 420–39

Sullivan, R. (1982). Europeans devise rapid method to determine if number is prime. *New York Times*, 5 February, A.16

Tapper, C. (1982). *Computer Law*, 2nd edition, Longman, Harlow

Ware, W.H. (1973). *Records, Computers and the Rights of Citizens*, US Government Printing Office, Washington, DC

Waring, L.P. (1978). *Management Handbook of Computer Security*, NCC, Manchester

Watne, D.A. and Turney, P.B.B. (1984). *Auditing EDP Systems*, Prentice-Hall, Englewood Cliffs, New Jersey

Watson, L. (1984). *A Systems Approach to Failures – Complexity, Management and Change*, Open University, Milton Keynes

Weissman, C. (1969). Security controls in the adept-50 time-sharing system. *Proceedings AFIPS Fall Jt Computer Conference*, Vol. 35, 119-33
Weissman, C. (1975). Secure computer operation with virtual machine partitioning. *AFIPS Conference, Proceedings* NCC, Vol. 44, 929-34
Westin, A. (1972). *Databanks in a Free Society: Computers, Record-keeping and Privacy*, Quadrangle Books, New York
WIPO (1978). *Model Provisions on the Protection of Computer Software*, Publication No. 814(E), International Bureau of the World Intellectual Property Organisation, Geneva
Wong, K.K. (1977). *Computer Security – Risk Analysis and Control*, NCC, Manchester
Wong, K.K. (1984). Data protection law. *Data Processing*, Vol. 26, No. 1, 34–7
Wood, H.M. (1977). The use of passwords for controlling access to remote computer systems and services. *AFIPS Conference, Proceedings NCC*, Vol. 46, 27-33
Wood, H.M. (1980). Computer based password techniques. In *Advances in Computer Security Management, Vol. 1* (ed. T.A. Rullo), Heyden, London, 141-67
Woodward, F. and Hoffman, L.J. (1974). Worst case costs for dynamic data element security decisions. *Proceedings ACM Conference*, 539–44

פרסומים אחרים באנגלית

Abrams, M D and Podell, H J / Computer and Network Security / IEEE computer society, 1987.
Baskerville, Richard / Designing Information Systems Security / John Wiley & Sons Inc, 1988.
Boling, M E / Personal Computer Security Software tools/ NTIS, 1988. DE88015320/WCC.
Cooper, James Arlin / Computer & Communications Security / McGraw-Hill Book Co., 1989.
Copyright Compliance for the Information Industry 1970-1989 / NTIS, PB89-860290/WLI.
Datapro Reports on Information Security / Datapro Research Corp., 1985-.
Data Security Management / Auerbach Publishers, 1982-.
Data Security Support Programs / IBM, 1985.
Fites, Philip; Johnston, Peter and Kratz, Martin / The Computer Virus Crisis / Van Nostrand Reinhold 1989.
Managing Microcomputer Security / FTP; 1987-.
NTIS Reports on Data Security, Computer Security, Microcomputers Security, Viruses Disaster Planning, on-line systems etc.
Pfleeger, Charles P / Security in Computing / Prentice-Hall, 1989.
Scott, Michael D / Computer Law / John Wiley & Sons, Inc, 1987.
Terry, P F and Wiseman, S R / Design and Implementation of a Secure Computer System / NTIS, AD-A201.

אינדקס ומילון מונחים

מערכות מידע ממוחשבות הן חלק בלתי נפרד מן הפעילות העסקית והמדעית בימינו. הנתונים המשמשים להן בסיס, הינם נכס של כל ארגון, כמו נכסים אחרים המאפשרים את השגת מטרותיו. פגיעה בהם, או בתהליכי העיבוד שלהם עלולה לגרום נזק רב לארגון. מסיבות אלו ואחרות, עלה נושא ההגנה על מערכות מידע לדרגת החשיבות הנוכחית.

המחבר מציג את הבעיות והקשיים שבאבטחת מידע ואת עקרונות האבטחה, ומציע שיטות להגנה על מערכות מידע ממוחשבות. הוא מנחה את הקורא כיצד לתכנן את מערכות הגנה הדרושות לארגון וכיצד לבדוק את יישומותן.

בין הנושאים בספר: אבטחה פיסית, בקרת כניסה, בקרה על בסיסי נתונים, הצפנה, פירטיות והצורך בהגנה על תוכנה, מערכות תקשורת ומערכות מקוונות, אנשים כמגינים וכפוגעים, הגנת מתקנים, אבטחה במחשבים אישיים והיבטים תפעוליים שונים.

הספר מסביר את החוק להגנת נתונים - הבסיס המשפטי לאבטחת מערכות מידע. ניתנים הסברים על ההתפתחות שהביאה לחקיקת חוקים לאבטחת מידע בבריטניה ובמדינות אחרות. מתוארים מקרים אחדים של פגיעה ומודגשים הלקחים שיש להפיק מהם.

ההיבט הישראלי של אבטחת מערכות המידע מוצג בנספח, שבו מאמר של עו"ד ג' אופנהיימר, הבהרות איל"א לחוק אבטחת הפרטיות, קווים מנחים לאבטחה של מאגרי מידע וחוק הגנת הפרטיות ותזכיר חוק המחשבים (עבירות, הגנת תוכנה וראיות). ניתנת גם סקירה על ניהול אבטחה במחשבים אישיים.

המחבר, **ו.פ. ליין** פרסם עבודות רבות בנושאי אבטחת מחשבים ובקרת מערכות פיננסיות. שימש יועץ למיחשוב, כיהן בתפקידי ניהול במערכות מחשוב והיה מנהל ומרצה ראשי של הפוליטכניק בצפון מזרח לונדון.

ISBN 965-361-010-4 מסת"ב